THE HONORABLE JAMES L ROBART

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

In Re: Zillow Group, Inc. Session Replay Software Litigation This Document Refers to: All Actions	Master File No. 2:22-cv-01282-JLR MICROSOFT CORPORATION'S MOTION TO DISMISS CONSOLIDATED AMENDED COMPLAINT NOTE ON MOTION CALENDAR: JUNE 30, 2023 ORAL ARGUMENT REQUESTED

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

TABLE OF CONTENTS

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

TABLE OF AUTHORITIES

Page(s)

CASES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

STATUTES

RULES

OTHER AUTHORITIES

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

I. INTRODUCTION

Plaintiffs' Consolidated Amended Complaint ("Compl.") is one in a recent rash of lawsuits (many filed by them) seeking to extend state wiretap statutes enacted decades ago to an online world these laws were never intended to regulate and to which these laws do not fit. They do so in an attempt to collect statutory damages from various website operators, like Zillow, and their third-party technology providers, like Microsoft, for website operators having a common type of analytics software called session replay software running on their websites. Session replay technology helps website owners analyze how users interact with their websites so the website operators can improve their sites. As acknowledged in the Complaint, such software undisputedly has "legitimate purposes," *id.* ¶ 34, and Microsoft's session replay technology, called Clarity, was designed to protect privacy and *avoid* collecting sensitive information, *see, e.g.*, *id*. ¶ 64 (acknowledging how Clarity masks text entered by users). Nonetheless, Plaintiffs argue that when they allegedly visited the Zillow website, they were subjected to a highly offensive intrusion upon their seclusion, and an unlawful "interception" of their communications under various state wiretapping statutes, which they claim entitle them to immense statutory damages.

In this case, Plaintiffs bring two claims against Microsoft on behalf of a putative, nationwide class for purported violations of (1) the Washington Privacy Act ("WPA"), RCW § 9.73.040 *et seq.* and (2) for invasion of privacy in violation of Washington common law. Plaintiffs also bring six claims in the alternative (if the Court finds Washington law does not apply nationwide) on behalf of several putative, state-level classes, for violation of (3) the Missouri Wiretap Act ("MWA"), Mo. Rev. Stat. § 542.400 *et seq.*; (4) the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630 *et seq*.; and for invasion of privacy in violation of the common law of (5) Illinois, and (6) Missouri.[1]

[1] Plaintiffs assert these and other claims against Zillow, which also fail as addressed in Zillow's motion to dismiss.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

The Court should dismiss Plaintiffs' claims under Rule 12(b)(6) with prejudice for the following reasons: (1) Plaintiffs fail to identify any "communication" necessary to support their State Wiretap Act claims; (2) they fail to show "interception" for varying, multiple reasons under each State Wiretap Act; and (3) they fail to plausibly allege intrusion of their seclusion that would be "highly offensive to a reasonable person" under state common law(s).

II. BACKGROUND

A. Microsoft Clarity

Microsoft's Clarity software, available to website owners, includes a session replay feature that can help website owners better understand how users engage with their websites. For example, Clarity is one way website owners can better understand what users click on and scroll through when they visit their websites, and it presents this information in a non-technical, easily understandable way—such as through website heatmaps that visualize where users tend to click on a page. Compl. ¶ 55.

This software is not directed to *who* is using a website; it is about *how* users do so. Microsoft takes common-sense steps to provide Clarity in a way that limits unnecessary collection of user data and protects user privacy. For example, as Plaintiffs recognize, Clarity customers (i.e., the website operators) can choose from among several "masking" options to avoid having information, like shipping addresses that people enter into text fields, collected or incorporated into Clarity's visualizations. *See* Compl. ¶ 64 n.43. The by-default "Balanced" masking means "sensitive text" is masked, including "all input box content," *see* Ex. 2; *see also infra* at 24 (discussing masking options in more detail). Additionally, the Clarity Terms of Use, which apply to all website operators that have Clarity on their websites, provide that Clarity can only be used "for analytics purposes such as experimenting on [customers'] website," prohibit

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

Microsoft customers from using Clarity "to create user profiles," and require compliance with all applicable laws and regulations such as data privacy laws.[2]

B. Zillow's Website

Plaintiffs allege Zillow procured third-party vendors, including Microsoft, to embed snippets of JavaScript computer code ("Session Replay Code"), such as Clarity, on Zillow's website (www.zillow.com and all of its subpages). *Id.* ¶¶ 1, 70.

According to Plaintiffs, Clarity collects the "Website Communications" of Plaintiffs and the putative class members they seek to represent. *See id.* ¶¶ 70, 110, 111. The term "Website Communications" is of Plaintiffs' own invention, and they have unilaterally defined it to include a Zillow website visitors' "mouse movements, finger swipes (for those who used their mobile phone and its web browser to interact with the website), clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time." Compl. ¶ 1. Plaintiffs allege that the supposedly captured user interactions can later "be translated into a simulation video of how a user interacts with a website" and used to evaluate and improve user engagement. *Id.* ¶¶ 1, 60–61.

While Plaintiffs allege that *other* session replay providers "indiscriminately capture the maximum" information possible, Plaintiffs concede that Microsoft does not do so. *Compare id.* ¶ 39, *with* ¶ 64. Instead of collecting all "keystrokes" entered by Zillow website visitors, Microsoft provides websites that use Clarity with three "masking" options: (1) "strict" masking, where all text on the website is masked (meaning none of it is collected); (2) "balanced"

[2] The Clarity Terms of Use are incorporated by reference in the Complaint and properly attached as Exhibit 1 because they are linked at https://learn.microsoft.com/en-us/clarity/faq, a website upon which Plaintiffs rely. *See* Compl. ¶ 58 n.36, ¶ 68 n.47 (citing URL that redirects to https://learn.microsoft.com/en-us/clarity/faq, which, in turn provides a direct link to https://clarity.microsoft.com/terms); *see also, e.g.*, *Bolling v. Dendreon Corp.*, 2014 WL 12042559, at *6 (W.D. Wash. Jan. 28, 2014) (Robart, J.) ("Where a plaintiff fails to attach to the complaint the documents upon which the complaint is premised, a defendant may attach such documents in order to show that they do not support the plaintiff's claim."). Alternatively, the Terms of Use are the proper subject of judicial notice. *See* Fed. R. Evid. 201(b); *Wilson v. Playtika, Ltd.*, 349 F. Supp. 3d 1028, 1042 (W.D. Wash. 2018).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

masking, where sensitive text—including all text input by a user—is masked; and (3) "relaxed" masking, where website operators can choose to unmask text input by their users. *See id.* ¶ 64. As explained in the very webpages cited by Plaintiffs in footnote 45 to paragraph 64 of their Complaint, the default setting is "balanced." *See id.* ¶ 64 n.45; Ex. 2; *see also supra* n.3. And so, unless Zillow affirmatively *changed* the masking settings— which Plaintiffs do not allege— "credit card information" and other sensitive information was masked. *See id.*

C. Plaintiffs' Alleged Interactions With The Zillow Website

Each of the nine named Plaintiffs in this action allege they "routinely visit[] Zillow's website to search for properties," but they do not allege *when* they visited the website beyond referencing the "years" "in" or "throughout" which they purportedly visited. Compl. ¶¶ 71–79. They admit they not only saw, but also were "relying on the Terms of Use of the [Zillow] website," Compl. ¶ 250, which incorporate Zillow's Privacy Policy.[3] That Privacy Policy, in turn, expressly discloses Zillow's use of session replay technology. Specifically, Zillow's Privacy Policy states in the "Information We Collect As You Use Our Services" section that it and its third-party providers "may collect certain personal data automatically when you visit or interact with our websites… [t]his includes things like your home search history, homes you view, purchase activity, what you've clicked on and other uses of our websites, and the amount of time you spend looking at different parts of our websites…" Ex. 3 at 2.

Instead of concrete allegations as to when Plaintiffs visited the Zillow site, which parts of the sites they viewed, which links the clicked, etc., the Complaint discusses at length *other*, unnamed, providers of session replay technology, consumer privacy surveys, and anonymous "website users" and "visitors." *See, e.g.*, Compl. ¶¶ 22–52. It then theorizes about the types of information that session replay technology *might* capture from *others* and the types of harms that *might* befall a hypothetical "website visitor" who engages with such technology. *Id.* ¶¶ 49–51.

[3] *See Terms of Use*, zillowgroup.com (Sept. 23, 2022), https://www.zillowgroup.com/terms-of-use ("See our [hyperlinked] Privacy Policy. . . .").

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

But Plaintiffs do not allege that *they* suffered such harms. *See Warth v. Seldin*, 422 U.S. 490, 499 (1975) ("[A named] plaintiff generally must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties.").

Plaintiffs Adams and H.A. allege only that they "substantively engaged with Zillow's website" and "entered information into text fields" without further elaboration—they do not describe the sorts of alleged "text fields" at issue. *See id.* ¶¶ 77–79. Other Plaintiffs also fail to elaborate about the context of their purported visits other than to identify the sorts of information they allegedly entered into text fields: such as names (all Plaintiffs *except* Adams and H.A.); physical addresses (Popa, Strezlin, Kauffman, Perkins, Hasson, and Huber); email address (Margulis only); and/or "offers to purchase properties" (Kauffman). *See id.* ¶¶ 71–79; *see also* App. A (table comparing allegations). Although the Complaint discusses how certain hypothetical websites deploying hypothetical session replay technology might, for example, capture "medical conditions" or "prescriptions," *id.* ¶ 50, Plaintiffs do not allege that the Zillow website requests such information or that it was captured by Clarity during Plaintiffs' visits.[4]

D. Plaintiffs' Claims

1. State Wiretap Acts

Plaintiffs' primary wiretapping claim, as well as two of their alternative claims, arise under state laws that were enacted in 1862 (CIPA),[5] 1967 (WPA), and 1989 (MWA), long before today's online experience, to prevent the interception and surreptitious recording of private telegraph and telephone conversations. Only one of these laws, CIPA, was amended to cover certain electronic communications technology. *See* Analysis of Sen. Bill No. 1428 (2009-2010 Reg. Sess.) (discussing purpose of 2010 amendment to CIPA to cover additional forms of

[4] The Microsoft Clarity Terms of Use prohibit website operators from using Clarity for health care data, providing: "You will not use the Offering in connection with content which may contain sensitive user materials, such as health care, financial services or government-related information." Ex. 1 § 1(b)(ii).

[5] The text of Section 631 was first introduced in California in 1862 under Cal. Penal Code § 640. *See* Statutes of California 1862, p. 288, CCLX II.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

electronic communications, namely "e-mail, blackberry, instant messaging by phone and other forms of contemporaneous two-way electronic communication"). But all three laws (collectively, the "State Wiretap Acts") remain intended to protect "communications" from surreptitious, non-consensual capture. RCW 9.73.030; Mo. Rev. Stat. § 542.402; Cal. Penal Code § 631. None of the State Wiretap Acts mention "Website Communications," Plaintiffs' unilaterally created term.

Each of the State Wiretap Acts has a unique scheme and elements. For instance:

- **WPA:** To state claims for "interception" of "private communications" under the WPA, Compl. ¶¶ 118–19, Plaintiffs must show that the "private" "communications" of "two or more individuals" were "intercepted" using a "device designed to record and/or transmit" without "consent from all parties," resulting in "injury." *See* RCW §§ 9.73.030, 9.73.060.
- **MWA:** To state claims for "interception" of a "wire communication" under the MWA, Compl. ¶¶ 222–23, Plaintiffs must show an "aural acquisition" of their "wire communications" using a "device" either without the consent of any party to the wire communication, or for a separate and independent "criminal or tortious purpose." Mo. Rev. Stat. § 542.402.
- **CIPA:** To state claims that Microsoft "intentionally taps" or "reads" a communication without consent under CIPA, Compl. ¶¶ 282–86, Plaintiffs must show that the allegedly collected data incudes the "content" of communications, that Microsoft had the requisite intent to violate CIPA, and that the alleged interception occurred while the communication was "in transit." Cal. Penal Code § 631(a).

All three State Wiretap Acts are criminal statutes, but Plaintiffs seek to invoke the civil provisions to obtain statutory damages.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

2. Common Law Privacy

Plaintiffs' remaining three claims against Microsoft are for common law intrusion of seclusion under Washington, or, alternatively, under Illinois or Missouri law. All three claims require Plaintiffs to allege facts plausibly showing (1) a private matter about which the plaintiff has a reasonable expectation of privacy, and (2) an unreasonable intrusion by defendant into that private matter (3) in a way that is highly offensive to a reasonable person. *See, e.g.*, *Crow v. Crawford & Co.*, 259 S.W.3d 104, 120 (Mo. Ct. App. 2008); *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004); *Gray v. Amazon.com, Inc.*, 2023 WL 1068513, at *8 (W.D. Wash. Jan. 27, 2023), *appeal filed*, No. 23-35377 (9th Cir. June 1, 2023).

In addition, under Washington law, a defendant must be "substantially certain" that they "lack[] the necessary legal or personal permission to commit the intrusive act." *Gray*, 2023 WL 1068513, at *8. And under Illinois law, the intrusion must cause actual anguish and suffering. *Schmidt v. Ameritech Ill.*, 768 N.E.2d 303, 316 (Ill. App. Ct. 2002).

Plaintiffs seek to bring these claims on behalf of a nationwide class of "all natural persons in the United States and its territories whose Website Communications were captured through the use of the Session Replay Code embedded in www.zillow.com," Compl. ¶ 100, and, alternatively (and as to Microsoft), on behalf of statewide subclasses of "all natural persons located in the states of California, Illinois, [and] Missouri," *id.* ¶ 101.

III. ARGUMENT

To survive a motion to dismiss under Rule 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, 'to state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). At the motion to dismiss stage, "[a]ll allegations of material fact are taken as true and construed in the light most favorable to the nonmoving party . . . . [but the] court [is not] required to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001), *opinion amended on denial of reh'g*, 275 F.3d 1187 (9th Cir. 2001). A

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

plaintiff must therefore plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678.

When construing state laws, this Court is bound by decisions of that state's highest court. *Blaylock v. First Am. Title Ins.*, 504 F. Supp. 2d 1091, 1101 (W.D. Wash. 2007) (Robart, J.). "If there is no controlling decision," then this Court "is obligated to predict how the highest state court would decide the issue using intermediate appellate court decisions, decisions from other jurisdictions, statutes, treatises, and restatements as guidance. In the absence of convincing evidence that the state supreme court would decide differently, a federal court must follow the decisions of the state's intermediate appellate courts." *Id.* (cleaned up).

A. Plaintiffs' State Wiretap Act claims fail because they did not "communicate" with Zillow.

Each of Plaintiffs' State Wiretap Act claims against Microsoft requires a threshold showing of a communication. The WPA prohibition invoked by Plaintiffs requires a "private communication," RCW 9.73.030(1)(a); their MWA claims require a "wire communication," Mo. Rev. Stat. § 542.402(1); and their CIPA claims hinge on "the contents or meaning of any message, report, or communication," Cal. Penal Code § 631(a). Yet none of these laws includes a statutory definition for "communication." Where a statute does not define a term, courts turn to the term's plain meaning and legislative intent. *See, e.g.*, *Wis. Cent. Ltd. v. United States*, 138 S. Ct. 2067, 2070 (2018) ("[O]ur job is to interpret the words consistent with their "ordinary meaning . . . at the time Congress enacted the statute."); *see also Olympic Tug & Barge, Inc. v. Wash. State Dep't of Revenue*, 355 P.3d 1199, 1201 (Wash. Ct. App. 2015) (recognizing same), *as amended on reconsideration in part on other grounds* (Aug. 18, 2015); *Ste. Marie v. Riverside Cnty. Reg'l Park & Open-Space Dist.*, 206 P.3d 739, 743 (Cal. 2009) (same); *Doe v. St. Louis Cmty. Coll.*, 526 S.W.3d 329, 336 (Mo. Ct. App. 2017) (same). These principles apply to the undefined term "communication." And under a plain meaning, "[t]he very concept of a 'communication' conveys the idea that *something* is communicated *to someone*." *State v. Ozuna*,

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

359 P.3d 739, 744 (Wash. 2015) (emphasis added) (citing dictionary definitions for plain meaning of "communication").

Plaintiffs' mouse movements and clicks are not "communications" under any plain reading of that term. They do not contain "a verbal or written message" to Zillow, do not "express []ideas effectively (as in speech)" to Zillow, and do not amount to an exchange of information between individuals (including because Zillow is not an "individual," *see infra* at 13). At best, they are simply actions taken by Plaintiffs to navigate and browse a website operated by Zillow, and Plaintiffs use the term "action" rather than communication to describe such conduct. *See, e.g.*, Compl. ¶¶ 34–36. One would not say, in ordinary conversation, that they "communicated" with Zillow by going to www.zillow.com and browsing properties. Even "entering" text into various text fields on the website, s*ee* Compl. ¶¶ 71–79, does not equate to *sending* a communication to a company—such as through a written email.

This foundational issue (along with others), helps explain why there is no case law under either the WPA or the MWA allowing claims to proceed based on use of session replay software like Clarity. *See In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1093 (N.D. Cal. 2015) (dismissing WPA claim based on collection of "user's geographical location, URLs, search terms, etc." through defendant's "network diagnostics tool" that was preinstalled on plaintiffs' cell phones). And it explains why so many courts have been skeptical of session replay cases under CIPA. For instance, in *Yoon v. Lululemon USA, Inc*., 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. 2021), the plaintiff alleged that a website's third-party software recorded her "keystrokes, mouse clicks, pages viewed, and shipping and billing information . . . [and] the date and time of the visit, the duration of the visit, Plaintiff's IP address, her location at the time of the visit, her browser type, and the operating system on her device." *Id.* at 1083. Still, the *Yoon* court concluded that "[n]one of these pieces of data constitutes message content" and dismissed plaintiffs California wiretapping claim. *Id.* Just as courts like *Yoon* recognized, this Court should also hold that Plaintiffs here are, at base, complaining that session replay technology allegedly tracked their

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

visit to a website. But even assuming that occurred, tracking actions to create an alleged "simulation video" of a user's web session is much more analogous to security footage than it is to the surreptitious gathering of the content of telephone conversations or email messages that legislatures were worried about when they passed and amended wiretap laws. *See*, *e.g.*, *Jacome v. Spirit Airlines Inc.*, 2021 WL 3087860, at *4 (Fla. Cir. Ct. June 17, 2021) (dismissing wiretap claims based on session replay technology after comparing it to movement tracking of the sort expressly *not* intended to be covered by wiretap); *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1319, 1321–22 (S.D. Fla. 2021) (same).[6] Plaintiffs do not plausibly allege interception or tapping of "communications" under the State Wiretap Acts, defeating these claims and requiring dismissal.

B. Plaintiffs' claims under the WPA fail for additional reasons.

The WPA states in relevant part:

> [I]t shall be unlawful for any individual, partnership, corporation, association, or the state of Washington . . . to intercept . . . any: . . . Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication.

RCW 9.73.030(1)(a) (emphasis added). Plaintiffs have failed to state a claim under the WPA because (1) they have not identified "two or more individuals" affected by Microsoft's purported interception; (2) they do not allege facts plausibly showing (a) "a private communication transmitted by a device," (b) that was "intercepted" (c) "by use of … a device designed to record and/or transmit," and (d) "without the consent of all parties to the private communication," *State v. Roden*, 321 P.3d 1183, 1186 (Wash. 2014) (*en banc*); and (3) Plaintiffs have not alleged facts

[6] The few cases holding otherwise are neither binding nor persuasive, as these courts failed to properly analyze the "communication" element of the wiretap claims. *See, e.g.*, *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503 (C.D. Cal. 2021) (court failed to analyze whether browsing a website equals communicating with it, making decision unpersuasive and unhelpful); *Revitch v. New Moosejaw*, LLC, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2021) (similar).

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

plausibly showing "a violation of [the] statute has injured [their] business . . . person or . . . reputation." RCW 9.73.060.

1. Plaintiffs' interactions with the Zillow website do not amount to communications "between two or more individuals"

The WPA prohibits the interception of private communications only where they occur "between two or more individuals[.]" RCW 9.73.030(1)(a). Plaintiffs may each be "individuals," but Zillow is not, and so Plaintiffs' WPA claims fail.

Indeed, this was the holding of *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012). One of the claims brought by the plaintiff there was that Microsoft violated the WPA by acquiring location data transmitted from her phone without consent. But the Court held that, unlike some other laws, "the WPA requires a communication between at least two individuals," *id.* at 1129, and Microsoft was not an individual. This holding is consistent with the plain meaning of "individual," *i.e.*, "a single human being as contrasted with a social group or institution." https://www.merriam-webster.com/dictionary/individual; *see also, e.g.*, *Roden*, 321 P.3d at 1186 (applying dictionary definition of "private" to the WPA in the absence of a statutory definition). It is also consistent with the sorts of person-to-person (as opposed to person-to-business) disputes that tend to arise under the interception prohibition of the WPA. *See, e.g.*, *State v. Bilgi*, 496 P.3d 1230, 1237 (Wash. Ct. App. 2021) (dismissing WPA interception claim involving criminal-to-victim communications), *review denied*, 504 P.3d 827 (Wash. 2022).

Because Zillow is not an "individual" and Plaintiffs do not allege private communications between them and any other individual, their WPA claim fails.

2. Plaintiffs' interactions with the Zillow website were not "private."

"Private" is not defined under the WPA, but "Washington courts have adopted the dictionary definition: 'belonging to one's self . . . secret . . . intended only for the persons involved (a conversation) . . . holding a confidential relationship to something . . . a secret

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

message: a private communication . . . secretly: not open or in public.' A communication is private (1) when parties manifest a subjective intention that it be private and (2) where that expectation is reasonable based on the duration and subject matter of the communication, the location of the communication, and the presence of potential third parties." *In re Hopper*, 424 P.3d 228, 231–32 (Wash. Ct. App. 2018) (cleaned up); *see also State v. Clark*, 916 P.2d 384, 394 (Wash. 1996) ("[T]he presence of one or more third parties . . . means that the conversations were not private in any ordinary or usual meaning of that word."). Here, even if Plaintiffs had communicated with other individuals, or even if their time on the Zillow website could be construed as communications, their claim would still fail because they allege no facts plausibly showing they subjectively intended for their supposed communications with a public website to be private. Nor can they claim ignorance as to the use of session replay technology when they allegedly visited www.zillow.com, *see, e.g.*, Compl. ¶ 133, as they are serial session replay litigants: five of them have filed ten other cases (nine of which were filed prior to or within mere months of this case) besides those now consolidated in this action, *see* App. B (table).

Second, even if Plaintiffs had alleged facts from which the Court could infer they subjectively intended their website browsing to be private, an expectation of privacy would not be reasonable here. Plaintiffs acknowledge that consumers expect their online activities to be tracked and shared. *See, e.g.*, Compl. ¶¶ 22–32. And here, the Zillow privacy policy specifically states, among other things, that Zillow:

> [M]ay use tracking technologies to automatically collect commercial information, preferences, and internet, network and device information, including: . . . . **Information about how you use the services**, such as the pages you visit, the links you click, the ads you view and click on, purchase information and your checkout process, your location when you access or interact with our services, and other similar actions . . . . **Analytics Data**, such as information about your activity when you visit our sites or use our apps; this can include clicks, mouse movements, forms you fill out, and similar information.

Ex. 3 at 2 Plaintiffs therefore cannot claim any reasonable expectation of privacy given Zillow's

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

obvious and disclosed practices. This is especially the case here given their concession that they were "relying on the Terms of Use of the [Zillow] website," Compl. ¶ 250, which incorporate the Privacy Policy that expressly discloses Zillow's use of session replay.

State v. Corliss, 838 P.2d 1149 (Wash. 1992), *aff'd*, 870 P.2d 317 (Wash. 1994), provides a helpful comparison. There, a police informant tipped a handheld telephone receiver to allow a police officer to overhear a defendant's conversation. *Id*. at 1150–51. The court of appeals held that this did not violate the WPA because, among other reasons, it was "doubtful there was a 'private communication', because [defendant] assumed the risk that [the other communicant] would allow someone else to listen—a circumstance that is not so odd or remarkable as to create in [defendant] an expectation of privacy that only one person would listen at the other end." *Id.* at 1151. Similarly, here, website users "assume the risk" that a website like Zillow will use "tracking technologies" provided by third parties, as expressly disclosed in Zillow's Privacy Policy. Thus, even if the Court reaches the "private" element of Plaintiffs' WPA claim (and it need not, as Plaintiffs do not allege "communications" in the first instance, much less with other individuals), it should find Plaintiffs fail to satisfy this essential element, requiring dismissal.

3. Plaintiffs' interactions with the Zillow website were not "intercepted."

To "intercept" under the WPA means to "stop . . . before arrival . . . or interrupt the progress or course." *Roden*, 321 P.3d at 1188 (cleaned up). Accordingly, courts have consistently held that "interception" within the meaning of the WPA must occur *prior* to receipt by the intended recipient. *See id.*; *see also, e.g.*, *Bilgi*, 496 P.3d at 1236 (applying *Roden* to hold that "interception" requires a "stop[] . . . before arrival . . . or interrupt[ion] the progress or course" of a communication); *State v. Ramos*, 2019 WL 4200596, at *5 (Wash. Ct. App. Sept. 5, 2019) (unpublished) (same). But Plaintiffs do not allege that Microsoft received any data from them *prior* to Zillow's receipt of that data.

On a motion to dismiss, factual allegations need to be accepted as true, but courts are "not bound to accept as true a legal conclusion couched as a factual allegation," or "conclusory

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

statements," or "a formulaic recitation of the elements of a cause of action." *Iqbal*, 556 U.S. at 677 (cleaned up). Here, Plaintiffs allege only that their data was transferred "at hyper-frequent intervals" and before their website visit was "completely finished," Compl. ¶ 35–36, and they assert that their "electronic communications are intercepted contemporaneously with their transmission." *Id.* ¶ 124. But these conclusory assertions do not suggest, and Plaintiffs do not even attempt to allege, that Microsoft "*stop[ped] . . . before* arrival . . . or *interrupt[ed]* the progress or course" of any communication or conversation. *Roden*, 321 P.3d at 1188 (emphasis added). For this reason, too, Plaintiffs fail to state a claim against Microsoft for interception under the WPA.

4. Clarity is not a "device" designed to record and/or transmit.

Plaintiffs' WPA claims also fail because Clarity is not a "device designed to record and/or transmit" RCW 9.73.030(1)(a). The WPA does not further define "a device designed to record and/or transmit." But courts have applied WPA only to *physical* devices like cell *phones* and *computers*. S*ee, e.g.*, *State v. Townsend*, 57 P.3d 255, 260 (Wash. 2002); *State v. Christensen*, 102 P.3d 789, 794 (Wash. 2004). Microsoft is not aware of any case applying the term "device" to non-physical software for the purpose of the WPA at all. This makes good sense, as the ordinary understanding of the word "device" is that a device is something physical: "a piece of equipment." *Device*, Merriam-Webster Dictionary (last visited May 17, 2023), https://www.merriam-webster.com/dictionary/device. The Court should dismiss Plaintiffs' WPA claims for the additional reason that Clarity is not a "*device* designed to record and/or transmit," and no allegation could change this outcome.

5. Plaintiffs consented to acquisition of their data.

Even if all that were otherwise (and it is not), consent to so-called interception would defeat Plaintiffs' WPA claims. Consent may be implied when the circumstances of the conversation make it clear that plaintiff knew or should have known about the defendant's alleged conduct. *See, e.g.*, *Townsend*, 57 P.3d at 260 (holding that plaintiff "is properly deemed

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

to have consented to the recording of [email] messages" given that email must necessarily be "recorded on the computer of the person to whom the message was sent"); *State v. Wright*, 2020 WL 6557814, at *5 (Wash. Ct. App. Nov. 9, 2020) (same as to text message). So too here. As discussed, Zillow's privacy policy disclosed the conduct of which Plaintiffs complain. *See supra* at 12–13; *see also* Zillow Mot. at § III.A.1. Plaintiffs' use of the Zillow website thus demonstrates implied consent, *especially* given that they are repeat session replay plaintiffs, *see* App. A (table), and admit they *relied* on Zillow's terms that incorporate the privacy policy, Compl. ¶ 250.

6. Plaintiffs' do not allege injury for purposes of the WPA.

Finally, Plaintiffs lack statutory standing to sue under the WPA because they have not plausibly alleged harm to their persons, business, or reputation as result of the alleged WPA violation, as the statute requires. A mere statutory violation is not enough for standing under the WPA; a plaintiff must also show "that a violation of [the] statute has injured his or her business, his or her person, or his or her reputation." RCW 9.73.060; *see, e.g.*, *Goussev v. Toyota Motor Sales, U.S.A., Inc.,* 2022 WL 1423642, at *4 (W.D. Wash. May 5, 2022) (denying WPA claim because "Plaintiffs' concerns that their data could be accessed in the future by a third party may or may not be justified . . . [and] the unknown future is insufficient to adequately plead injury under the WPA"); *Russo v. Microsoft Corp.*, 2021 WL 2688850, at *3 (N.D. Cal. June 30, 2021) (finding statements "that [defendant] used and shared" data "far too sparse and conclusory to make the claim of personal injury plausible"); *Brinkley v. Monterey Fin. Servs., LLC*, 340 F. Supp. 3d 1036, 1044-45 (S.D. Cal. 2018) (dismissing WPA claim for lack of actual financial damages).

The WPA does not specify the standard for injury to "person," but no court has held that bare mental injury of the kind Plaintiffs allege suffices under WPA. A plaintiff's allegation of mental injury must be objectively reasonable: "the reaction of a normally constituted person." *Hunsley v. Giard*, 553 P.2d 1096, 1103 (Wash. 1976). A court may make this determination as a

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

matter of law. *Id.* Conclusory allegations that a plaintiff "suffered humiliation, mental anguish, emotional, and physical distress" are insufficient, and "[t]he court need not accept these generalized allegations as true." *Caldwell v. Boeing Co.*, 2018 WL 2113980, at *10 (W.D. Wash. May 8, 2018); *see also Iqbal*, 556 U.S. at 678; *Samia v. Experian Info. Sols., LLC*, 2022 WL 298369, at *3 (S.D. Cal. Feb. 1, 2022) (dismissing plaintiff's claims following identity theft in part because plaintiff failed to plead facts to support allegations that he "suffered emotional distress and damage to his credit worthiness").

Here, Plaintiffs cite to the WPA's injury requirement but do not adequately plead any injury to a person, reputation, or business, much less as a result of the alleged conduct. *See* Compl. ¶¶ 116–27. They assert that they have suffered "mental anguish," "emotional distress," worry, fear, and "suffering arising from their loss of privacy and confidentiality of their electronic communications," Compl. ¶¶ 138–39, but they offer no factual support to explain how or show these mental injuries are objectively reasonable. Plaintiffs' lack of resulting injury thus provides yet another reason to dismiss their WPA claims with prejudice.

C. Plaintiffs' claims under the MWA fail for additional reasons.

Plaintiffs also allege that Microsoft has "intercepted" the "contents" of their "wire communications" using an "electronic, mechanical, or other device" in violation of the MWA. Compl. ¶¶ 232–34. The MWA provides in relevant part:

> [A] person is guilty of a class E felony and upon conviction shall be punished as provided by law, if such person: (1) [k]nowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire communication [unless] . . . such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act.

Mo. Rev. Stat. § 542.402.1(1); *id.* § 542.402.2(3). Plaintiffs therefore must allege facts plausibly showing actual or attempted (1) interception of (2) their wire communication (3) without consent. They do not.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

1. Plaintiffs fail to allege "interception."

"Intercept" is defined in the MWA as "the *aural* acquisition of the contents of any wire communication through the use of any electronic or mechanical *device*." Mo. Rev. Stat. § 542.400(6) (emphasis added). Therefore, to state a claim under the MWA, Plaintiffs must allege "aural" acquisition (of a "wire communication") through the use of a "device." They fail to do so.

The term "aural" is undefined in the statute, meaning a Missouri court would apply its ordinary meaning "of or relating to the ear or to the sense of hearing." *aural*, Merriam-Webster Online Dictionary (last visited May 15, 2023), https://www.merriam-webster.com/dictionary/aural. Plaintiffs allege Microsoft captured their online activity, which they allege consisted of "mouse clicks and movements, keystrokes, search terms, information inputted . . . and pages and content click on and viewed by Plaintiffs." Compl. ¶ 95. None of this describes any captures of *audible* data, squarely defeating Plaintiffs' MWA claims. *See United States v. Gregg*, 829 F.2d 1430, 1434 (8th Cir. 1987) (holding there is no "aural" acquisition where interception "does not involve hearing sounds of the voice" under the analogous Federal Wiretap Act where the MWA derives this language).

Second, they do not allege the use of a "device." The MWA defines "device" as "any device or apparatus which can be used to intercept a wire communication." Mo. Rev. Stat. § 542.400(5). Missouri courts have applied this definition according to its ordinary meaning: "a piece of equipment or a mechanism designed to serve a special purpose or perform a special function."[7] And so Missouri courts have held, for example, that an answering machine or voice-activated recording device plugged into a phone line is a "device" under the MWA. *Carothers v. Carothers*, 977 S.W.2d 287, 290 (Mo. Ct. App. 1998). In these Missouri cases, the "special purpose" or "special function" of these devices were, understandably, to make "aural

[7] *Device*, Merriam-Webster Dictionary (last visited May 17, 2023), https://www.merriam-webster.com/dictionary/device.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

acquisition" of spoken communications. *See Carothers*, 977 S.W.2d at 290; *State v. Martinelli*, 972 S.W.2d 424, 431-32 (Mo. Ct. App. 1998). There does not appear to be any Missouri case holding non-tangible software is a "device" under the MWA, much less that software *not* designed for "*aural acquisition*" is a "device." Because Plaintiffs allege neither "aural acquisition" nor "device," they fail to allege "interception," and their MWA claim fails for this reason too.

2. Plaintiffs' data is not a "wire communication."

Plaintiffs also fail to plausibly allege the interception of a "wire communication" because that term applies only to communications via common carrier telephone services and does not encompass the type of website activity Plaintiffs allege. The MWA was never intended to apply to even "electronic communications," as Plaintiffs allege (Compl. ¶ 236), much less to Plaintiffs' self-invented term "Website Communications." When the Missouri legislature passed the MWA in 1989, it adopted much of the language from the federal Wiretap Act, 18 U.S.C. § 2510 *et seq*. In fact, the definition of "wire communications" in the MWA is nearly verbatim to a now-outdated definition in the Federal Wiretap Act:

> any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate communications.

Mo. Rev. Stat. § 542.400(12); *see also* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801(a), 82 Stat. 197, 213) (1968) (defining "wire communication" nearly verbatim); *Phillips v. Am. Motorist Ins.*, 996 S.W.2d 584, 588 (Mo. Ct. App. 1999) (holding the MWA was modeled after the Federal Wiretap Act).

Before the MWA was passed in 1989, Congress recognized that the above definition of "wire communication" was limited to traditional common carrier telephone services, and so amended the federal Wiretap Act by passing the Electronic Communications Privacy Act, Pub.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

L. No. 99-508, 100 Stat. 1848 ("ECPA") in 1986 to protect the new forms of highly analogous communicative technology that were being used "in lieu of, or side-by-side with, first class mail and common carrier telephone services," such as email and voice transmissions over fiber optic cable. S. Rep. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559; 18 U.S.C. §§ 2510-2523 (1986). When the Missouri legislature enacted the MWA three years later, it chose *not* to adopt ECPA's new definition for "electronic communications" and instead chose *only* to adopt the old prohibition on the interception of "wire communications" (which Congress recognized applied only to traditional common carrier telephone services). Mo. Rev. Stat. § 542.400 (1989). And so, Plaintiffs are simply wrong to assert that the MWA protects "electronic communications," much less their website browsing. Compl. ¶ 236. In short, Plaintiffs cannot state MWA claims based on the alleged interception of "electronic communications" when the Missouri legislature chose not to adopt that language in the statute. *See id.*

3. Plaintiffs' MWA claims fails due to party consent.

Plaintiffs' MWA claims fail for the additional, independent reason that the MWA only requires one-party's consent to the alleged "interception," and Plaintiffs admit that Zillow, a party to the conversation, consented to the use of Clarity. *See e.g.*, Compl. ¶ 1 (alleging that Zillow "procures" Microsoft Clarity). By alleging that Zillow consented to Clarity, Plaintiffs plead themselves out of their MWA claim, since they acknowledge consent of a party (Zillow) to the alleged interception. Mo. Rev. Stat. § 542.400(6) (emphasis added); Mo. Rev. Stat. § 542.402.2(3).

Plaintiffs' MWA claims fail for this reason unless they plausibly allege the recordings were made for a "tortious purpose." *See* Mo. Rev. Stat. § 542.402.2(3). To meet this element, plaintiffs must allege "the defendant . . . [has] the intent to use the illicit recording to commit a tort or crime beyond the act of recording itself . . . . Intent may not be inferred simply by demonstrating that the intentional act of recording itself constituted a tort." *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 144-45 n.81 (3d Cir. 2015) (discussing

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

similar requirement in the Federal Wiretap Act) (citation omitted); *compare* 18 U.S.C. § 2511(2)(d) (describing crime-tort exception), *with* Mo. Rev. Stat. § 542.402.2(3) (same). But Plaintiffs have only alleged state wiretapping and common law intrusion upon seclusion claims, all of which merely allege "the intentional act of recording itself" and not any separate tortious purpose. *See, e.g.*, Compl. ¶ 2 (alleging use of Clarity to recreate web visits), 62 (alleging use of Clarity to create heatmaps). Indeed, not only do Plaintiffs fail to allege *any* "tortious purpose" for Microsoft's alleged actions, but also Plaintiffs acknowledge that websites use session replay technology for "some legitimate purposes." *Id.* ¶ 34. Because Plaintiffs admit a party to the supposed interception consented to it, their MWA claims fail.

D. Plaintiffs' claims under CIPA fail for additional reasons.

Plaintiffs' last State Wiretap Act claim against Microsoft is for "wiretapping" and "interception" of the "contents" of "communications" in violation of CIPA, Compl. ¶¶ 277, 290, which provides:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner**,** [1] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [2] who **willfully** and **without the consent** of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the **contents** or meaning of any **message, report, or communication while the same is in transit or passing over any wire, line, or cable,** or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine [or jail time].

Cal. Penal Code § 631(a) (emphasis added); *see also Mastel v. Miniclip*, 549 F. Supp. 3d 1129, 1134 (E.D. Cal. 2021) (describing distinction between operative clauses of CIPA). Plaintiffs do not state a CIPA claim because they (1) do not allege telegraph or telephone equipment (to the

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

extent they invoke the first clause of Section 631); (2) do not allege facts showing the "contents" of any of their communications were intercepted; (3) do not allege the requisite willful intent by Microsoft; and (4) fail to satisfy the "in transit" requirement.

1. To the extent Plaintiffs invoke the first clause of Section 631, that theory fails due to the absence of telegraph or telephone equipment.

"Courts have consistently interpreted [the first] clause [of CIPA] as applying only to communications over telephones and not through the internet." *Licea v. Cinmar, LLC*, 2023 WL 2415592, at *5 (C.D. Cal. Mar. 7, 2023); *see also Williams v. What If Holdings, LLC*, 2022 WL 17869275, at *2 (N.D. Cal. Dec. 22, 2022) (determining "the first clause of Section 631(a) concerns telephonic wiretapping specifically, which does not apply to the context of the internet"). This is because, "under the rule of ejusdem generis, where general words follow an enumeration of specific items, the general words are read as applying only to other items akin to those specifically enumerated." *Harrison v. PPG Indus.*, 446 U.S. 578, 588 (1980). And so, under the first clause of Section 631, the terms "wire," "line," "cable" and "instrument" in Section 631 are all initially modified by the words "telegraph" and "telephone." It is thus not enough to allege that Clarity accesses data through a wire, line, cable, or instrument without also identifying telephone equipment—especially given that CIPA is a criminal statute, because "[I]n construing criminal statutes the ejusdem generis rule of construction is applied with stringency." *People v. Thomas*, 156 P.2d 7, 17 (Cal. 1945). Plaintiffs do not allege any such telephone equipment and so to the extent they seek to assert a claim under the first clause of section 631 of CIPA, that effort fails.

2. Plaintiffs do not plausibly allege that the "contents" of any communications are at issue.

As explained above, *see supra* at 10–13, Plaintiffs do not allege facts showing they "communicated" with Zillow at all but rather that they navigated and browsed the Zillow

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

website. Plaintiffs also have not shown that Clarity captured the "*contents or meaning* of any message, report, or communication." Cal. Penal Code § 631(a) (emphasis added).

"The 'contents' of a communication under CIPA and the federal Wiretap Act are the same." *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 833 (N.D. Cal. 2021). Namely, contents are "the intended message conveyed by the communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Contents do not include "record information regarding the characteristics of the message that is generated in the course of the communication" such as "the name, address and subscriber number or identity of a subscriber or customer." *Id.* (cleaned up). In the Internet context, contents include things like the body of email messages sent among friends. By contrast, the URL of a webpage viewed by a given user is not content, *id.* at 1107–09, nor is an IP address, username, or location information, *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1085 (N.D. Cal. 2018), *on reconsideration on other grounds*, 2018 WL 3068248 (N.D. Cal. June 21, 2018), or "data on when and how often an Android Smartphone user opens and runs non-Google apps and the amount of time spent on the apps," *McCoy v. Alphabet, Inc.*, 2021 WL 405816, at *14 (N.D. Cal. Feb. 2, 2021) (interpreting CIPA).

Here, Plaintiffs allege that they "routinely visit[] Zillow's website." Compl. ¶¶ 71–79. These allegations support the inference that Plaintiffs typed "www.zillow.com" into a browser bar, clicked enter—and, *possibly*, scrolled and clicked on the website. But it is well established that entering a URL into a browser bar merely facilitates use of a website—it does not amount to communication content. *See In re Zynga Priv. Litig.*, 750 F.3d at 1109; *In re Nickelodeon Consumer Priv. Litig.*, 2014 WL 3012873, at *15 (D.N.J. July 2, 2014) (recognizing a URL is used to "identify the physical location of documents on servers connected to the internet" and is thus unlike "the spoken words of a telephone call") (cleaned up). The same is true of visits to multiple subpages—i.e., website browsing, since this is again URL information. *Id.* And courts agree that "[m]ouse movements and clicks [and] scrolling and window resizing," FAC ¶ 53, are all actions that merely facilitate the use of a website and do not reveal the substance of any

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

communication. *See, e.g.*, *Yoon*, 549 F. Supp. 3d at 1082–83 (holding under federal and California wiretap law that "mouse clicks" and "pages viewed" do not "constitute[] message content in the same way that the words of a text message or an email do"); *Goldstein*, 559 F. Supp. 3d at 1319, 1321–22 (rejecting "novel reading of Florida's decades-old wiretapping statute" of "creative class action litigants" and holding that "mouse clicks and movements," "scroll movements," and "pages and content viewed" do not "not convey the substance of any communication"); *see also, e.g.*, *Jacome*, 2021 WL 3087860, at *4 (holding that "mouse clicks and movements" and "pages and content viewed by Plaintiff" were "precisely the type of . . . information that courts consistently find do not constitute 'contents' under the Federal Wiretap Act or any of its state analogs because it does not convey the substance or meaning of any message"). Indeed, website browsing information about where a cursor moved and when is akin to non-content information about a telephone call, "such as the call's time of origination and its duration." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (cleaned up).

Plaintiffs' allegations regarding entering text into various fields or text boxes on Zillow's website cannot save their claims. First, user inputs into name, email, and address fields still amount to non-content "record" information about the user as opposed to communications from the user—"whether automatically generated or not." *Yoon*, 549 F. Supp. 3d at 1082–83; *see also In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1034 (N.D. Cal. 2014) ("email content" is content for wiretapping statutes, but "name, address, email address or phone number" are not). The same is true of any credit card information, which is analogous to the sort of "billing" information that law enforcement can obtain with a subpoena because it is non-content. *See, e.g.*, *Chevron Corp. v. Donziger*, 2013 WL 4536808, at *2, *6 (N.D. Cal. Aug. 22, 2013) (holding billing information was non-content under the Federal Wiretap Act); *Svenson v. Google Inc.*, 2015 WL 1503429, at *7 (N.D. Cal. Apr. 1, 2015) (collecting cases distinguishing "content" from "record information"

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

under the Federal Wiretap Act).[8] Indeed, the plaintiff in *Yoon* alleged a website's third-party software collected, among other things, her "shipping and billing information," but the Court concluded that "[n]one of the[] pieces of data [identified by the plaintiff] constitutes message content." *Yoon*, 549 F. Supp. 3d at 1083.

Second, even if it were plausible to infer that Plaintiffs typed some *communicative* message into the Zillow website (and it isn't), there is no allegation from which it could be inferred that such material was not at least partially masked from Clarity. Plaintiffs correctly acknowledge that "Clarity offers websites three standard approaches when it comes to masking sensitive information collected from a user's interactions with a website[.]" Compl. ¶ 64. Plaintiffs mischaracterize the masking modes however. In truth, the by-default "Balanced" masking means "[o]nly sensitive text is masked," and **all input box content**, numbers, and email addresses [are classified] **as sensitive text**." *See* Ex. 2. This means that under the default setting of Clarity, neither Microsoft nor Zillow collected any user-inputted text using Clarity. *See id.* Plaintiffs have not—and cannot—plead any facts showing this default setting was ever changed by Microsoft or Zillow. At bottom, Plaintiffs' allegations amount to the assertion that Clarity tracked their non-content virtual movements and user commands on the Zillow website, but under settled law, that does not suffice to state a claim under CIPA. *See supra* at 22–23.

3. Microsoft lacks the requisite intent for a violation of Section 631.

Section 631 of CIPA requires a showing that the defendant "intentionally" or "willfully" engaged in wiretapping. Cal. Penal Code § 631(a). Plaintiffs fail to allege facts plausibly showing this level of culpability by Microsoft.

Microsoft is unaware of any decisions interpreting the "intentional" or "willful" standard under Section 631. But similar language appears in Section 632, which prohibits "intentional" eavesdropping on "confidential communications," and that standard was discussed in *Vartanian*

[8] Moreover, financial information is not collected under Clarity's default setting, which Plaintiffs do not allege Zillow ever changed. Compl. ¶ 64.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

v. VW Credit, Inc., 2012 WL 12326334, at *2 (C.D. Cal. Feb. 22, 2012). The plaintiff there alleged that his customer service calls were recorded without his knowledge or consent, but the court dismissed the claim because the plaintiff failed to plausibly allege that the defendant *knew* the customer service calls were "confidential." *Id.* at *3; *see also People v. Superior Ct.*, 449 P.2d 230, 238 (Cal. 1969) (requiring "purpose or desire of recording a confidential conversation" or "substantial certainty that his use of the equipment will result in the recordation of a confidential conversation"). Similarly here, it is not enough to allege Microsoft intended to deploy session replay technology; plaintiffs must allege facts from which the Court could plausibly infer that Microsoft intended to capture "communications." Plaintiffs' own complaint makes clear that Microsoft did not intend to do that, because Plaintiffs' allegations show Microsoft has no control over Zillow's website or the activities that users engage in on that website; Microsoft requires its customers to comply with all privacy laws and prohibits websites from using Clarity to collect, e.g., financial data; and Microsoft established masking procedures to enable its website customers to avoid capturing "sensitive information" that customers like Zillow, not Microsoft, control. Compl. ¶ 64; *see also supra* at 5–6. Plaintiffs do not allege the requisite intent, warranting dismissal of their CIPA claims for this additional reason.

4. Plaintiffs do not plausibly allege data was collected while in "transit."

To state a CIPA claim, Plaintiffs must allege that Clarity captures data while "in transit or passing over any wire, line or cable." Cal. Penal Code § 631(a). Plaintiffs assert their "electronic communications were in transit or passing over any wire, line, or cable" when captured, Compl. ¶ 286, and that "user information [is] collected in real time and recorded by Clarity," *id.* ¶ 61. But these conclusory allegations need not be accepted as true, and the Court should reject them for the same reasons as those in *Hammerling v. Google LLC*, 2022 WL 17365255, at *10 (N.D. Cal. Dec. 1, 2022). There, the plaintiffs alleged that "Google secretly used their Android smartphones to collect data regarding their use of third-party apps," such as by collecting "real-time data" about one of the plaintiff's visits to a shopping app. *Id.* at *10. But the Court

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

dismissed the CIPA claim for the simple reason that "real-time data" could be sent to Google by the app operator *after* the operator's real-time collection. And "Plaintiffs [did] not plausibly allege any mechanism that would allow Google [to collect the data in real-time itself]." *Id.*; *see also Bradley v. Google*, Inc., 2006 WL 3798134, at *6 (N.D. Cal. Dec. 22, 2006) ("[CIPA] require[s] the interception of an electronic communication. [Plaintiff] has not alleged that Google intercepted her communications, only that her stored emails were deleted from her account"); *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1227–28 (C.D. Cal. 2017) (dismissing where plaintiffs made only conclusory allegations of the purported interception during transmission); *Rosenow v. Facebook, Inc.*, 2020 WL 1984062, at *7–8 (S.D. Cal. Apr. 27, 2020) (same).

So too here. Plaintiffs do not plausibly allege any facts to show Clarity collected data in transit. To the contrary, Plaintiffs allege that Clarity sends "a packet of event response data" in (albeit very short) increments *after* collection. Compl. ¶ 85. Their CIPA claims should thus be dismissed for the same reasons as in the above cases.

E. The rule of lenity prohibits Plaintiffs from stretching the State Wiretap Acts to Microsoft here.

Even if all that were otherwise (and it is not), the State Wiretap Acts are at least ambiguous here on essential elements—i.e., the meanings of "intercept," "private," "contents," and "in transit." And so the rule of lenity bars Plaintiffs' claims against Microsoft.

Each of the State Wiretap Acts is a criminal statute, and "[t]he rule of lenity applies where two possible constructions of a criminal statute are permissible." *State v. Phelps*, 77 P.3d 678, 680 (Wash. Ct. App. 2003); *United States v. Millis*, 621 F.3d 914, 917 (9th Cir. 2010) (applying rule of lenity to question of whether leaving one-gallon plastic bottles of purified water intended for consumption by undocumented immigrants violated the prohibition against leaving "garbage" behind at a federal wildlife refuge). The rule of lenity requires courts "to favor a more lenient interpretation of a criminal statute when, after consulting traditional canons of statutory

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

construction, we are left with an ambiguous statute." *Kasten v. Saint-Gobain Performance Plastics Corp.*, 563 U.S. 1, 16 (2011) (cleaned up); *see also State v. Graham*, 204 S.W.3d 655, 656 (Mo. 2006) (*en banc*) (holding that "ambiguity in a penal statute will be construed against the government or party seeking to exact statutory penalties and in favor of persons on whom such penalties are sought to be imposed"); *Harrott v. County of Kings*, 25 P.3d 649, 659 (Cal. 2001) (rule of lenity applies to "resolving any ambiguity in the ambit of [a criminal] statute's coverage" when "the language or history of [a statute] is uncertain" to "ensure both that there is fair warning of the boundaries of criminal conduct and that legislatures, not courts, define criminal liability"). This is true even where private litigants like Plaintiffs are seeking to enforce the civil provisions, because the same definitions are incorporated into its criminal prohibitions as well. *See* RCW 9.73.030, 9.73.060; Cal. Penal Code §§ 631, 637.2; Mo. Rev. Stat. §§ 542.402, 542.418.

Here, even if this Court were to disagree with Microsoft's interpretations, the State Wiretap Acts fall well short of the "clear and definite" language necessary to give "fair notice" that they might punish the use of non-physical Clarity code to analyze website interactions to improve user engagement. *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) ("If there is any doubt about whether Congress intended to prohibit the conduct engaged, then we must choose the interpretation least likely to impose penalties unintended by Congress.") (cleaned up). The list of terms the WPA leaves undefined and potentially ambiguous in RCW 9.73.030(1) alone includes: "private," "communication," "conversation," "device," "individuals," "between points," "consent," and "engaged." CIPA is similarly opaque, with "intent," "line, cable, or instrument," "tapped," "unauthorized connection," and "content," among other terms. *See* Cal. Penal Code § 631. The MWA does not apply to Plaintiffs' allegations (*see infra* at 16–20), but to find otherwise would require interpreting the undefined term "aural acquisition" and "wired communications," a defined term almost verbatim to the one Congress deemed too narrow to include email and even wireless telephones, to apply to website data for the first time (*id.*). And

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

because it is *at best* debatable whether those terms extend to Microsoft's Clarity given the interpretive issues already discussed, the novel interpretation pressed by Plaintiffs risks "unintentionally turn[ing] ordinary citizens into criminals." *Nosal*, 676 F.3d at 863.

Legislative history also undermines Plaintiffs' over-reaching. The WPA and MWA were passed in the mid-twentieth century, and CIPA Section 631's predecessor a century earlier. To apply these ambiguous statutes to technology that legislators could not have begun to contemplate is the essence of unfairness and unpredictability the rule of lenity seeks to prevent. And that remains true notwithstanding amendments made to the WPA and CIPA, because those amendments still focus on communications *analogous to* the sorts of telephone conversation that those laws were originally intended to protect (like emails). *See supra* at 7–8. There is no reason to believe that—had the Legislature foreseen the use of technology like session replay—it would have required prior consent to its use to avoid criminal violations. Indeed, interpreting the State Wiretap Acts as Plaintiffs suggest would lead to the absurd result of requiring providers and website operators to potentially collect *more* information about website visitors to determine which state they are located in, and then obtain consent from them to understand what they are doing on their website, through a web banner or pop-up screen, lessening the user experience on the website. The State Wiretap Acts were not intended to produce this result.

This case is similar to *Gray v. Twitter Inc.*, 2021 WL 11086642 (W.D. Wash. Mar. 17, 2021), where the court considered a statute that criminally barred the unauthorized sale or procurement of telephone records, and which defined "telephone record" as "information *retained by* a telecommunications company that relates to the telephone number dialed by the customer or the incoming number or call directed to a customer, or other data related to such calls typically contained on a customer telephone bill such as the time the call started and ended, the duration of the call, the time of day the call was made, and any charges applied." *Id.* at *4 (emphasis added) (quoting RCW 9.26A.140(5)(b)). The plaintiff there alleged that Twitter used deceptive practices to procure his telephone number from him, thus making it "unauthorized"

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

and violating the statute. But the court concluded that the rule of lenity required the statute to be construed in favor of Twitter, holding that "because a customer's telephone number is not expressly included in the definition of telephone record, under the rule of lenity, it is not a telephone record." *Id.* at *9 (internal quotations omitted). So too here, because "mouse clicks and movements," "keystrokes," and "search terms" do not appear in the State Wiretap Acts—and because such data was not on the radar of the original drafters and has not been addressed by any subsequent amendment—the rule of lenity applies.

Similarly, in *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022), the court considered whether plaintiff's scraping of LinkedIn's freely accessible website, after it received a cease-and-desist letter from LinkedIn, meant that access was "without authorization" for purposes of the Computer Fraud and Abuse Act ("CFAA"). *Id.* at 1200–01. The court noted that "data scraping is a common method of gathering information, used by search engines, academic researchers, and many others," *id.* at 1201, and that the legislative history showed the intention to prohibit conduct "analogous to that of 'breaking and entering,'" *id.* 1196. The court then applied the rule of lenity to narrowly interpret the "without authorization" provision of the CFAA to not apply to websites that are made freely accessible on the internet "so as not to turn a criminal hacking statute into a sweeping internet-policing mandate." *Id.* (internal quotations omitted). So too here, accepting Plaintiffs' efforts to extend the Wiretap Acts to technology that was not on the legislature's radar when it passed or amended those laws.

In the absence of a clear intention of the relevant state legislatures to criminalize the commonplace and innocuous conduct at issue here, the rule of lenity applies to prevent the State Wiretap Acts from being stretched to apply without proper notice to Microsoft, and by proxy, the entire session replay industry.

F. Plaintiffs have not plausibly alleged intrusion upon seclusion.

All of Plaintiffs' primary (Washington) and alternative (Illinois and Missouri) common law claims alleged against Microsoft share some core elements: all generally require (1) a private

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

matter that the plaintiff has a reasonable expectation of privacy over, and (2) an unreasonable intrusion by a defendant into that private matter (3) in a way that is highly offensive to a reasonable person. *See, e.g.*, *Crow*, 259 S.W.3d at 120; *Busse*, 813 N.E.2d at 1017; *Gray*, 2023 WL 1068513, at *8. Plaintiffs do not meet these elements. Nor do they meet the additional requirement under Washington law that any intrusion must be "deliberate," *Gray*, 2023 WL 1068513, at *8, or that they suffered actual anguish and suffering under Illinois law, *Schmidt*, 768 N.E.2d at 316.

1. Plaintiffs' alleged visits to the Zillow website are not a private matter in which they had a reasonable expectation of privacy.

Plaintiffs allege to have entered—to varying degrees—the following sorts of information into the Zillow website: names, addresses, birth dates, phone numbers, and credit card numbers. But courts regularly find this sort of information to be insufficiently private in nature to form the basis for an intrusion upon seclusion claim. *See, e.g.*, *Busse*, 813 N.E.2d at 1017 (finding that "names, telephone numbers, addresses or social security numbers" of customers are not private facts, unlike *truly* private facts like "family problems, romantic interests, sex lives," and so forth). Moreover, the most "sensitive" information at issue here, "credit card[] and other financial information," Compl. ¶¶ 71–79 (alleged only by some Plaintiffs); *see also* App. B, could not have been collected under Clarity's default masking settings, which were the default masking settings and which Plaintiffs do not allege Zillow (or Microsoft) ever changed. *See supra* at 24. In any event, this is not the sort of information over which one has a reasonable expectation of privacy over when sharing with a website online. *See, e.g.*, *Popa v. Harriet Carter Gifts*, *Inc.*, 426 F. Supp. 3d 108, 122 (W.D. Pa. 2019) (holding "keystrokes, mouse clicks, and PII [personally identifiable information]" of Plaintiff Popa that was allegedly collected by a technology similar to session replay when she visited a different website was insufficient to state an intrusion upon seclusion claim under analogous Pennsylvania law), *vacated on other grounds*, 52 F.4th 121 (3d Cir. 2022). And Plaintiffs acknowledge that "a majority of Americans,

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

approximately 79%," are aware that information concerning their online activities is collected. *See* Compl. ¶ 31; *id.* n.12 (citing 2019 Pew Research Center survey). Under these circumstances, it simply would not be reasonable for a website user to consider their mouse movements, clicks, and text inputs with the Zillow website as a "private matter."

That is especially true here, as Plaintiffs subjectively knew about session replay technology: indeed, over half of them filed similar claims based on similar technology in other cases before they filed this case. *See supra* at 11–12. But what's more, Plaintiffs allege they were "relying on the Terms of Use of the [Zillow] website," Compl. ¶ 250, which incorporate the Privacy Policy.

2. Any intrusion by Microsoft was not "unreasonable."

Regardless, even if Plaintiffs had a reasonable expectation of privacy in their interactions with the Zillow Website, Plaintiffs' have not shown any "unreasonable" intrusion.

Again, Plaintiffs admit they relied on Zillow's Terms of Use and those terms disclosed the use of technology like Clarity. Compl. ¶ 251. It was therefore reasonable for Microsoft's Clarity software to be used as it was on Zillow's website. Plaintiffs are simply *wrong* to suggest that such use of Clarity would only be "reasonable" if they gave express consent. *See, e.g.*, *Gray*, 2023 WL 1068513, at *8 (dismissing intrusion upon seclusion claim under Washington law where Plaintiffs "were on notice of" privacy policies, even if they did not click to view or agree to those policies); *see also Jacome*, 2021 WL 3087860, at *7 (finding defendant's website's privacy policy put plaintiffs on inquiry notice of website's use of session replay).

But notice isn't the only issue for Plaintiffs. Their objection to Microsoft's so-called intrusion is also undermined by Clarity's default masking policies, which they admit prevent the collection of potentially sensitive user data. *See supra* at 24. For this reason, too, even if Microsoft had committed any intrusion (and it did not), that would have been reasonable because it was disclosed and Microsoft took steps to prevent the collection of sensitive data.

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

3. The alleged intrusion is not "highly offensive" to a reasonable person.

For the same reasons, any purported intrusion was not highly offensive. "Courts have recognized facts sufficient to satisfy the "highly offensive" element of intrusion of seclusion in the context of repeated phone calls, eavesdropping on workplace conversations, and unauthorized email review," *In re Google, Inc. Priv. Pol'y Litig.*, 58 F. Supp. 3d 968, 987 (N.D. Cal. 2014), but not in regard to commonplace tracking of internet activity. For example, "using cookies to track children was not highly offensive" under state law in *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 262 (3d Cir. 2016). In *Boring v. Google Inc.*, 362 F. App'x 273, 276, 279 (3d Cir. 2010), photographing plaintiffs' residence and swimming pool from a vehicle in their residence's driveway, which required passing a "Private Road, No Trespassing" sign to reach, has not highly offensive because "[n]o person of ordinary sensibilities would be shamed, humiliated, or have suffered mentally as a result of a vehicle entering into his or her ungated driveway and photographing the view from there." Disclosing a user's LinkedIn ID and the URLs of all of the LinkedIn profile pages the user viewed was not highly offensive (*Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal., 2012)), neither was collecting user data and browser histories, (*In re Google, Inc. Priv. Pol'y Litig.*, 58 F. Supp. 3d at 988), or collecting app usage data on mobile phones (*Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1090 (N.D. Cal. 2022)). If using cookies to track children online, collecting app usage data from mobile phone users, and photographing peoples' homes from public streets is not "highly offensive," neither is the common use of session replay technology to understand how users interact with a realty website. *See, e.g.*, *id.* ("data collection and disclosure to third parties that is 'routine commercial behavior' is not a 'highly offensive' intrusion of privacy").

For these very reasons, one of the Plaintiffs (Popa) has *already* been rebuffed in her intrusion-upon-seclusion theory under analogous Pennsylvania law. *See Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d at 122 ("collecting Popa's keystrokes, mouse clicks, and [personally identifiable information] is simply not the type of highly offensive act to which liability can

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

attach" for common law intrusion upon seclusion) (collecting cases); *see also, e.g.*, *In re Nickelodeon*, 827 F.3d at 295 n.205 (whether an alleged intrusion is "highly offensive" may be decided as a matter of law). Plaintiffs' intrusion upon seclusion claims here fail for the same reasons.

4. Plaintiffs' do not allege Microsoft was "substantially certain" it lacked Plaintiffs' consent for Zillow to use Clarity on its website.

Plaintiffs' Washington common law claims also fail for the independent reason that they fail to allege that Microsoft believed or was "substantially certain" Plaintiffs had not consented to Zillow using Clarity during Plaintiffs' alleged visits to the Zillow website. Under Washington law, "[a]n actor commits an intentional intrusion only if he believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act." *Gray*, 2023 WL 1068513, at *8 (no requisite intent where Amazon had obtained permission to record plaintiffs' voices); *see also Poore-Rando v. United States*, 2017 WL 576871, at *2 (W.D. Wash. 2017) (holding there is no intrusion under Washington law when one "reasonably believed that [their] presence was supported by the necessary legal or personal permission"). Here, Zillow's Terms of Use (on which Plaintiffs rely, Compl. ¶ 250) incorporates the privacy policy that discloses the use of Clarity. That, combined with the fact that Microsoft requires customers to use Clarity consistent with local laws, *supra* at 25, prevent any inference that Microsoft was substantially certain that Plaintiffs had not provided sufficient consent here.

5. Plaintiffs' Illinois intrusion upon seclusion claims fail for the additional reason that they do not allege an actual injury.

Finally, Plaintiffs' Illinois common law claims fail for the additional reason that they fail to allege actual injury. "Under Illinois law, a plaintiff must prove actual injury in the form of, for example, medical care, an inability to sleep or work, or a loss of reputation and integrity in the community in order to recover damages for torts such as intrusion upon seclusion. Injury is not

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

presumed." *Schmidt*, 768 N.E.2d at 316 (cleaned up). As already explained as to the "injury" requirement of the WPA, *see supra* at 14–16, Plaintiffs fail to adequately allege injury here.

IV. CONCLUSION

For the foregoing reasons, Microsoft respectfully requests that the Court dismiss Plaintiffs' complaint against it with prejudice.

Dated: June 6, 2023

By: /s/ *James G. Snell*

Nicola C. Menaldo (SBN WA 44459)
Anna Mouw Thompson (SBN WA 52418)
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000
NMenaldo@perkinscoie.com
AnnaThompson@perkinscoie.com

James G. Snell (SBN CA 173070)
Perkins Coie LLP
3150 Porter Drive
Palo Alto, California 94304-1212
Telephone: 650.838.4300
Facsimile: 650.838.4350
JSnell@perkinscoie.com

Attorneys for Defendant Microsoft Corporation

APPENDIX A

The below table summarizes the categories of information that each named Plaintiff alleges to have "entered" while visiting the Zillow website. *See* Compl. ¶¶ 71-79. Even if true, however, the materials incorporated by reference in Plaintiffs' complaint and attached to Microsoft's motion as Exhibit 2 explain how "Clarity masks all sensitive content on your website by default. The sensitive content includes *all input box content*, [as well as] numbers, and email addresses [whether in an input box *or elsewhere*]. Clarity doesn't capture masked content." Ex. 2 at 1 (emphasis added).

Category of Information	Perkins	Hasson	Huber	Kauffman	Popa	Strezlin	Margulis	H.A.	Adams
Name	x	x	x	x	x	x	x		
Address	x	x	x	x	x	x			
Email Address							x		
Phone Number	x	x	x	x	x	x			
Date of Birth	x	x	x		x	x			
Credit Score Range	x	x	x						
Current Loans	x		x						
Estimate of Loans	x		x						
"Other Financial Information"		x							

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

APPENDIX B

The below table lists the other session replay litigation filed by named Plaintiffs.

Plaintiff	Other session replay litigation
Hasson	*Hasson v. Parts ID, Inc.*, No. 22-cv-01291 (W.D. Pa. Sept. 8, 2022) *Hasson v. FullStory, Inc.*, No. 22-cv-01246 (W.D. Pa. Aug. 30, 2022)
Huber	*Huber v. Expedia Grp.*, Inc., No. 22-cv-03570 (E.D. Pa. Sept. 7, 2022) *Huber v. Lowe's Cos.*, No. 22-cv-03571 (E.D. Pa. Sept. 7, 2022)
Kauffman	Kauffman v. Alaska Airlines, Inc., No. 22-cv-01525 (S.D. Cal. Oct. 6, 2022) Kauffman v. Am. Airlines, Inc., No. 22-cv-01524 (S.D. Cal. Oct. 6, 2022), *transferred* 22-cv-01123 (N.D. Tex. Dec. 19, 2022) *Kauffman v. Home Depot, Inc.*, No. 23-cv-0259 (S.D. Cal. Feb. 10, 2023)
Popa	*Popa v. PSP Grp., LLC*, No. 2:22-cv-1357 (W.D. Pa. Sept. 22, 2022), *transferred* 23-cv-00294-JLR (W.D. Wash. Mar. 10, 2023) *Popa v. Harriet Carter Gifts, Inc.*, No. 10248-19 (Pa. C.P.), *removed* 2:19-cv-00450 (W.D. Pa. Apr. 19, 2019), *appealed* No. 21-2203 (3d Cir. June 23, 2021)
Adams	*Adams v. PSP Grp., LLC*, No. 4:22-cv-01210-RLW (E.D. Mo. Nov. 14, 2022)

Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Phone: +1.206.359.8000
Fax: +1.206.359.9000

EXHIBIT 1

MICROSOFT CLARITY - TERMS OF USE

PLEASE READ THE "BINDING ARBITRATION AND CLASS ACTION WAIVER" SECTION BELOW. IT AFFECTS HOW DISPUTES ARE RESOLVED.

These Microsoft Clarity Terms of Use (these "**Terms**") are an agreement between You and Microsoft Corporation (or one of its affiliates) ("**Microsoft**"). They apply to Microsoft's Clarity service (the "**Offering**"), and any updates to the Offering (except to the extent such updates are accompanied by new or additional terms, in which case those different terms apply prospectively and do not alter Your or Microsoft's rights relating to a pre-updated version of the Offering). As used in these Terms and unless separately identified as applicable to either an individual or entity, "You" and "Your" refer to both you individually and the entity on behalf of which You are entering into these Terms.

BY CLICKING THE "ACCEPT" BUTTON"" OR OTHERWISE ACKNOWLEDGING YOUR ACCEPTANCE OR USING THE OFFERING, YOU (A) ACCEPT THESE TERMS AND AGREE THAT YOU ARE LEGALLY BOUND BY ITS TERMS; AND (B) REPRESENT AND WARRANT THAT: (I) YOU ARE 18 YEARS OF AGE; AND (II) IF YOU ARE ENTERING INTO THESE TERMS ON BEHALF OF A CORPORATION, GOVERNMENTAL ORGANIZATION, OR OTHER LEGAL ENTITY, YOU HAVE THE RIGHT, POWER, AND AUTHORITY TO ENTER INTO THESE TERMS ON BEHALF OF SUCH ENTITY AND BIND SUCH ENTITY TO ITS TERMS. IF YOU DO NOT AGREE TO THESE TERMS, MICROSOFT WILL NOT AND DOES NOT LICENSE TO YOU OR OTHERWISE GIVE YOU ACCESS OR USE RIGHTS WITH RESPECT TO THE OFFERING, AND YOU MUST NOT DOWNLOAD, INSTALL, OR OTHERWISE USE THE OFFERING.

1. **INSTALLATION AND USE RIGHTS.**
   a) General. Subject to Your ongoing compliance with these Terms, Microsoft gives You a nonexclusive, nontransferable, nonsublicensable, revocable and limited right to access and use the Offering for internal business purposes.
   b) **Use Requirements.** Your use of the Offering is subject to the following, and You warrant to Microsoft the same:
      i. You will use the Offering solely for analytics purposes such as experimenting on Your website and A/B testing. You will not use the Offering to create user profiles.
      ii. You will not use the Offering in connection with content which may contain sensitive user materials, such as health care, financial services or government-related information.
      iii. You will comply with all applicable laws, rules and regulations related to Your access and use of the Offering, including but not limited to privacy and security laws (as detailed further in Section 4).
   c) **Third Party Software.** The Offering may include third party applications that Microsoft or the applicable third party offers You under these Terms as part of the Offering. Your use of such third party applications is subject to full compliance with the applicable terms of such third party applications.
   d) **Open Source Components.** The Offering may contain third party copyrighted software licensed under open source licenses with source code availability obligations. Copies of those licenses are included in the "ThirdPartyNotices" file or other accompanying notices file.
2. **TERM AND TERMINATION.**
   a) **Term.** These Terms are effective on Your acceptance and may be terminated by Microsoft in its sole discretion for any or no reason per Section 9, "Changes to the Offering." Microsoft may extend these Terms in its discretion.
   b) **Access to data.** You may not be able to access data used in the Offering when it stops running or when these Terms terminate.
3. **FEEDBACK.** If You give feedback about the Offering to Microsoft, You give to Microsoft, without charge, the right to use, share and commercialize Your feedback in any way and for any purpose. You will not give feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because Microsoft includes Your feedback in them. These rights survive these Terms.
4. **DATA PROTECTION.**
   4.1. **Definitions.**
      a) "Controller" means the natural or legal person, public authority, agency or any other bodywhich alone or jointly with others determines the purposes and means of the Processing of Personal Data.
      b) "Data Protection Law" means any law, rule, regulation, decree, statute, or other enactment, order, mandate or resolution, applicable to You or Microsoft, relating to data security, data protection and/or privacy, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and the free movement of that data ("GDPR"), and any implementing, derivative or related legislation, rule, regulation, and regulatory guidance, as amended, extended, repealed and replaced, or re-enacted.
      c) "Personal Data" means any data or information that constitutes personal data or personal information under any applicable Data Protection Law, including any information relating to a natural person.
      d) "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.
      e) "Processing" means any operation or set of operations that is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction. "Process" and "Processed" will have a corresponding meaning.
      f) "Sensitive Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
   4.2. **Description of the Data Processing Activities.**
      a) Subject Matter of the Processing: Information, including Personal Data, that the parties Process in connection with the Offering.
      b) Duration of the Processing: The parties will Process Personal Data consistent with the duration of these Terms.
      c) Nature and Purpose of the Processing: The Offering will enable You to analyze the activity and characteristics of Your websites and users of Your websites, for example, capturing data about user mouse movements and performance data about specific web pages.
      d) Type of Personal Data Implicated by the Processing: The Offering assigns a unique user ID to each user. Any information associated with that user ID is Personal Data. Microsoft may collect statistical data about Your use of the Offering.
      e) Categories of Individuals Affected by the Processing: Individuals who access Your websites that have integrated the Offering. The parties may also Process the Personal Data of their respective employees in the course of using the Offering.
   4.3. Data Security. With respect to confidential information, including Personal Data, and any aggregated data that the parties may create from Personal Data, the parties will implement reasonable physical, technical, and organizational security controls to prevent or mitigate the effect of a breach of security that could or did cause the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, such confidential information or aggregate data. When the parties choose security controls, they will take into account the state of the art; cost of implementation; the nature, scope, context, and purposes of Personal Data Processing; and the risk to individuals of a security incident or breach affecting confidential information or aggregate data.
   4.4. Data Processing Obligations.
      a) Compliance with Law. The parties will comply with Data Protection Law.
      b) Privacy Policies. Each party will maintain a privacy notice that complies with Data Protection Law, and such privacy notice will effectuate, and take into account, these Terms. Your privacy notice will disclose that third parties such as Microsoft may collect Personal Data from individuals visiting Your websites and offer appropriate opt-out choices as required by Data Protection Law. You will disclose in your privacy notice the fact that Microsoft collects or receives Personal Data from you to provide Microsoft Advertising, and provide a link to the Microsoft Privacy Statements: https://privacy.microsoft.com/en-us/privacystatement.
      c) Status of the Parties; Data Uses.
         i. You and Microsoft are independent Controllers of the Personal Data Processed in connection with the Offering. The parties agree that neither of them are a "processor," "service provider," or equivalent status under Data Protection Law in connection with the Offering. The parties agree that they are independently responsible under Data Protection Law for the Personal Data they may receive from each other in connection with their performance of these Terms.
         ii. You will not knowingly disclose Personal Data that includes Sensitive Data to Microsoft.
         iii. Microsoft may use the Personal Data it collects in connection with the Offering for any purpose in accordance with the Microsoft Privacy Statement, including to provide the Offering; improve Microsoft's products and services, including reporting and performance analysis; and create user profiles for purposes that include advertising. Microsoft may also use nonpersonal data it collects in connection with the Offering to provide and improve Microsoft's products and services.
      d) Lawful Basis of Processing. To the extent that You are required by Data Protection Laws to have a lawful basis of Processing Personal Data, such as consent or legitimate interests, Your Processing of Personal Data will be consistent with that lawful basis. If Your lawful basis of Processing is consent, You will obtain consent consistent with applicable Data Protection Law and the scope of the consent you obtain will enable Microsoft to use the Personal Data it collects for the purposes

URL

https://clarity.microsoft.com/terms

Timestamp

Tue Jun 06 2023 11:41:16 GMT-0700 (Pacific Daylight Time)

to individuals of a security incident or breach affecting confidential information or aggregate data.

4.4. Data Processing Obligations.

a) Compliance with Law. The parties will comply with Data Protection Law.

b) Privacy Policies. Each party will maintain a privacy notice that complies with Data Protection Law, and such privacy notice will effectuate, and take into account, these Terms. Your privacy notice will disclose that third parties such as Microsoft may collect Personal Data from individuals visiting Your websites and offer appropriate opt-out choices as required by Data Protection Law. You will disclose in your privacy notice the fact that Microsoft collects or receives Personal Data from you to provide Microsoft Advertising, and provide a link to the Microsoft Privacy Statements: https://privacy.microsoft.com/en-us/privacystatement.

c) Status of the Parties; Data Uses.

i. You and Microsoft are independent Controllers of the Personal Data Processed in connection with the Offering. The parties agree that neither of them are a "processor," "service provider," or equivalent status under Data Protection Law in connection with the Offering. The parties agree that they are independently responsible under Data Protection Law for the Personal Data they may receive from each other in connection with their performance of these Terms.

ii. You will not knowingly disclose Personal Data that includes Sensitive Data to Microsoft.

iii. Microsoft may use the Personal Data it collects in connection with the Offering for any purpose in accordance with the Microsoft Privacy Statement, including to provide the Offering; improve Microsoft's products and services, including reporting and performance analysis; and create user profiles for purposes that include advertising. Microsoft may also use nonpersonal data it collects in connection with the Offering to provide and improve Microsoft's products and services.

d) Lawful Basis of Processing. To the extent that You are required by Data Protection Laws to have a lawful basis of Processing Personal Data, such as consent or legitimate interests, Your Processing of Personal Data will be consistent with that lawful basis. If Your lawful basis of Processing is consent, You will obtain consent consistent with applicable Data Protection Law and the scope of the consent you obtain will enable Microsoft to use the Personal Data it collects for the purposes described in this Section. For example, for individuals in the European Union, you must obtain consent for your use of cookies or other local storage, retain records of consent, and provide individuals with a clear means to revoke consent.

e) Cooperation. The parties will make commercially reasonable efforts to assist each other, upon request, to make information available necessary to demonstrate compliance with Data Protection Law, respond to inquiries from governmental entities, and respond to requests from individuals to exercise rights afforded to them under Data Protection Law.

f) Security Incidents. You will notify Microsoft without undue delay upon becoming aware of a Personal Data Breach affecting the Personal Data in connection with these Terms.

4.5. Conflict with Other Data Protection Terms. To the extent you have entered into a separate Microsoft Advertising Agreement, in the event of any conflict between this Agreement and the Microsoft Advertising Agreement, these Terms will prevail.

5. SCOPE OF LICENSE. The Offering is licensed, not sold. Microsoft reserves all other rights. You will not (and have no right to):
   a) work around any technical limitations in the Offering that only allow You to use it in certain ways;
   b) reverse engineer, decompile or disassemble the Offering;
   c) remove, minimize, block, or modify any notices of Microsoft or its suppliers in the Offering;
   d) use the Offering in any way that is against the law or to create or propagate malware; or
   e) share, publish, distribute, or lend the Offering, provide the Offering as a stand-alone hosted solution for others to use, or transfer the Offerings or this agreement to any third party.
6. EXPORT RESTRICTIONS. You must comply with all domestic and international export laws and regulations that apply to the Offerings, which include restrictions on destinations, end users, and end use. For further information on export restrictions, visit http://aka.ms/exporting.
7. SUPPORT SERVICES. Microsoft is not obligated under these Terms or otherwise to provide any support services for the Offering. Any support provided is "as is", "with all faults", and without warranty of any kind.
8. UPDATES. The Offerings may periodically check for updates, and download and install them for You. You may obtain and will use updates only from Microsoft or authorized sources. You agree to receive these automatic updates without any additional notice. Updates may not include or support all existing Offering features, services, or peripheral devices.
9. CHANGES TO THE OFFERING. Microsoft may change (including by removing features, adding or removing source types, or charging additional fees for features previously provided free or at different rates), update, enhance or modify the Offering at any time and may require You to obtain and use the most recent versions. Modifications may affect your ability to use the Offering and may require You to change (at Your sole cost) the way You previously used it. If any modification is unacceptable to You, Your only recourse is to stop using the Offering. Your continued use of the Offering following any update or change to the Offering will constitute Your binding acceptance to the update or change. Microsoft will not be liable for any costs that You incur, or for lost profits or damages of any kind related to any such modification. Microsoft may cancel or suspend Your use of the Offering or our provision of the Offering partially or in its entirety at any time. Microsoft's cancellation or suspension may be without cause, without notice, or both. Upon cancellation, Your right to use the Offering will cease immediately.
10. FEES AND PAYMENTS. Microsoft may charge fees for use of or access to some or all of the Offering. If Microsoft decides to charge, or charge additional or lesser fees for the Offering, such fees and additional terms and conditions will be disclosed to You prior to the effective date when such fees or requirements would be imposed. If You do not agree to such modifications, then You must stop using the Offering. If You do not stop using the Offering, Your use of the Offering will continue under the modified contract.
11. YOUR RESPONSIBILITY. You will indemnify and hold Microsoft (and its directors, officers, affiliates, and agents) harmless from and against any and all loss, liability, and expense (including reasonable attorneys' fees and costs) suffered or incurred by reason of any claims, proceedings, or suits based on or arising out of any breach (or alleged breach) by You of these Terms or any part of it, or that otherwise relates to Your website(s), Your application(s), or Your use of the Offering. You are responsible to defend any claim using mutually-agreed counsel, subject to Microsoft's right to participate with counsel it selects, and You will not publicize any claim or agree to any settlement that imposes any obligation or liability on Microsoft (or its directors, officers, affiliates, and agents) without Microsoft's prior written consent, such consent provided by Microsoft in its sole discretion.
12. BINDING ARBITRATION AND CLASS ACTION WAIVER. If You and Microsoft have a dispute, You and Microsoft agree to try for 60 days to resolve it informally. If You and Microsoft can't, You and Microsoft agree to **binding individual arbitration before the American Arbitration Association** under the Federal Arbitration Act ("FAA"), and **not to sue in court in front of a judge or jury**. Instead, a neutral arbitrator will decide. **Class action lawsuits, class-wide arbitrations, private attorney-general actions**, and any other proceeding where someone acts in a representative capacity **are not allowed**; nor is combining individual proceedings without the consent of all parties. The complete Arbitration Agreement contains more terms and is at http://aka.ms/arb-agreement-1. You and Microsoft agree to these terms.
13. ENTIRE AGREEMENT. These Terms, and any other terms Microsoft may provide for supplements, updates, or third-party applications, is the entire agreement for the Offering, and supersede all other oral and written agreements and understandings with respect to the Offering. Microsoft may make changes to these Terms by providing notice to You, which may be via email or posting a revised Terms of Use on its website or otherwise. Your continued use of the Offering after Microsoft provides You sufficient notice pursuant to the preceding sentence constitutes Your binding acceptance of such revised Terms of Use.
14. APPLICABLE LAW AND PLACE TO RESOLVE DISPUTES. You will comply with all applicable laws, regulations and ordinances. The laws of the state of Washington, U.S.A. govern the interpretation of these Terms, claims for its breach, and all other claims (including consumer protection, unfair competition, and tort claims), regardless of conflict of laws principles, except that the FAA governs everything related to arbitration. You and Microsoft consent to exclusive jurisdiction and venue in the federal court in King County, Washington for all disputes heard in court (excluding arbitration).
15. CONSUMER RIGHTS; REGIONAL VARIATIONS. These Terms describe certain legal rights. You may have other rights, including consumer rights, under the laws of Your state, province, or country. These Terms do not change those other rights if the laws of Your state, province, or country do not permit it to do so.
16. DISCLAIMER OF WARRANTY. THE OFFERING AND ANY DOCUMENTATION RELATED THERETO PROVIDED OR MADE AVAILABLE BY MICROSOFT IS PROVIDED ON AN "AS IS" AND "WHERE-IS" BASIS, WITH ALL FAULTS AND DEFECTS. YOU ACKNOWLEDGE THAT YOU BEAR THE FULL AND SOLE RISK OF USING THE OFFERING. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MICROSOFT HEREBY DISCLAIMS ALL WARRANTIES, GUARANTEES, OR CONDITIONS, EXPRESS OR IMPLIED WITH RESPECT TO THE OFFERING OR THE SUBJECT MATTER OF THESE TERMS, INCLUDING ALL IMPLIED WARRANTIES, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.
17. LIMITATION ON AND EXCLUSION OF DAMAGES. IF YOU HAVE ANY BASIS FOR RECOVERING DAMAGES DESPITE THE PRECEDING DISCLAIMER OF WARRANTY, YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. $5.00. IN NO EVENT WILL MICROSOFT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE OFFERING OR THESE TERMS.

This limitation applies to (a) anything related to the Offering, content (including code) on third party Internet sites, or third party applications; and (b) claims for breach of contract, warranty, guarantee, or condition; strict liability, negligence, or other tort; or any other claim; in each case to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to You because Your state, province, or country may not allow the exclusion or limitation of incidental, consequential, or other damages.

URL

https://clarity.microsoft.com/terms

Timestamp

Tue Jun 06 2023 11:41:16 GMT-0700 (Pacific Daylight Time)

PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

17. LIMITATION ON AND EXCLUSION OF DAMAGES. IF YOU HAVE ANY BASIS FOR RECOVERING DAMAGES DESPITE THE PRECEDING DISCLAIMER OF WARRANTY, YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. $5.00. IN NO EVENT WILL MICROSOFT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE OFFERING OR THESE TERMS.
This limitation applies to (a) anything related to the Offering, content (including code) on third party Internet sites, or third party applications; and (b) claims for breach of contract, warranty, guarantee, or condition; strict liability, negligence, or other tort; or any other claim; in each case to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to You because Your state, province, or country may not allow the exclusion or limitation of incidental, consequential, or other damages.

18. CONFIDENTIAL INFORMATION. The Offering, including its user interface, features and documentation, is confidential and proprietary to Microsoft and its suppliers.
   a) Use. For five years after installation of the Offering, You may not disclose confidential information to third parties. You may disclose confidential information only to Your employees and consultants who need to know the information. You must have written agreements with them that protect the confidential information at least as much as these Terms.
   b) Survival. Your duty to protect confidential information survives these Terms.
   c) Exclusions. You may disclose confidential information in response to a judicial or governmental order. You must first give written notice to Microsoft to allow it to seek a protective order or otherwise protect the information. Confidential information does not include information that:
      i. becomes publicly known through no wrongful act;
      ii. You received from a third party who did not breach confidentiality obligations to Microsoft or its suppliers; or
      iii. You developed independently without use of Microsoft's confidential information.
   d) Marketing. You agree that Microsoft may reference You and your marks and logos as a user of the Offering in a case study, press release, or on its website or other marketing collateral, without Your prior written consent, or any other obligation or accounting to You. You may withdraw your consent to this section (18(d)) by sending an email to: ClarityMS@microsoft.com.
   e) Publicity. You will not communicate with the press or public regarding the Offering without Microsoft's prior written consent.
19. SURVIVAL. The following sections of these Terms survive termination: 2, 3, 4, 6, 7, and 11-19.

URL

https://clarity.microsoft.com/terms

Timestamp

Tue Jun 06 2023 11:41:16 GMT-0700 (Pacific Daylight Time)

EXHIBIT 2

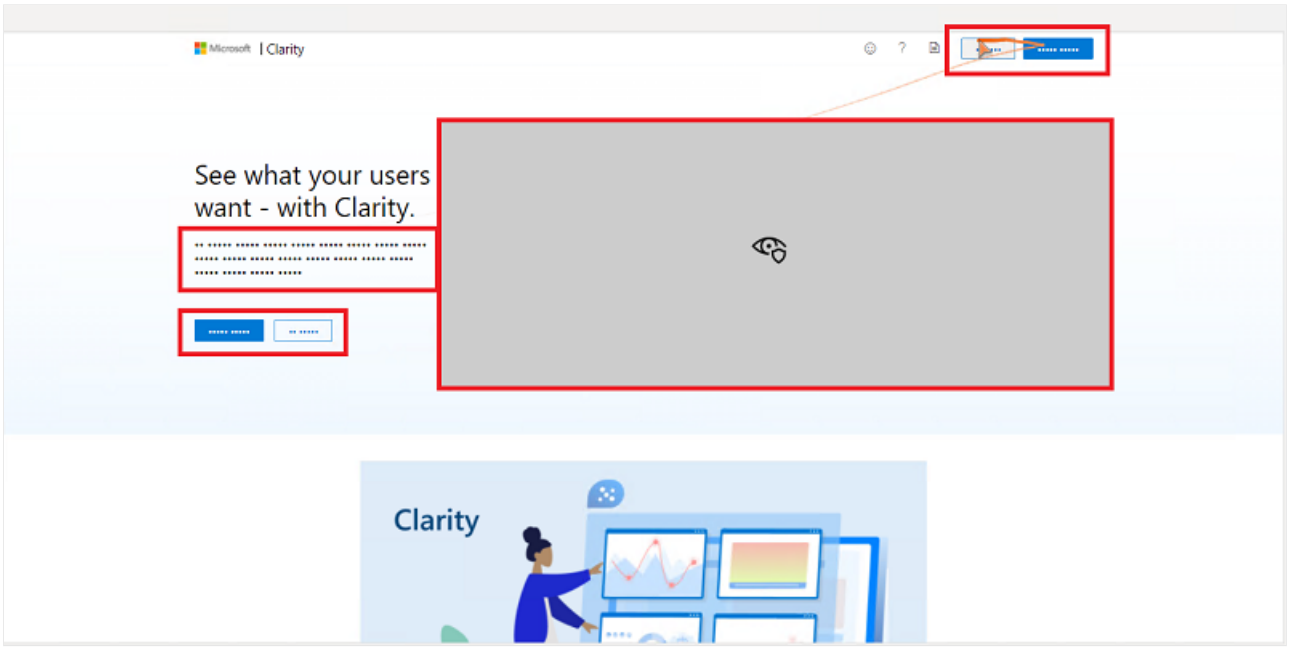
Masking Content

Article • 07/18/2022 • 3 minutes to read

Choose what Clarity can track on your website, either by masking or unmasking it. Masking is essential when your website may capture users' data that you don't want Clarity to store. When you choose to hide specific sites' data, you can keep your users' information private. The masking ensures it's never uploaded to Clarity.

Clarity masks all sensitive content on your website by default. The sensitive content includes all input box content, numbers, and email addresses. Clarity doesn't capture masked content.

Here's an example of how masked content is seen for text and images:



> **Note**
>
> Changes to masking settings affect new recordings and could take up to one hour to be reflected. Masking changes can't be applied retroactively.

How to mask and unmask content?

> **Note**
>
> Only a project's administrators can mask and unmask content. Members who are not admins can't edit the masking mode, add, or delete mask elements.

Masking and unmasking can be done in many ways:

- Using the Clarity website
  - Masking modes - Choose a mask mode that applies to your entire site.

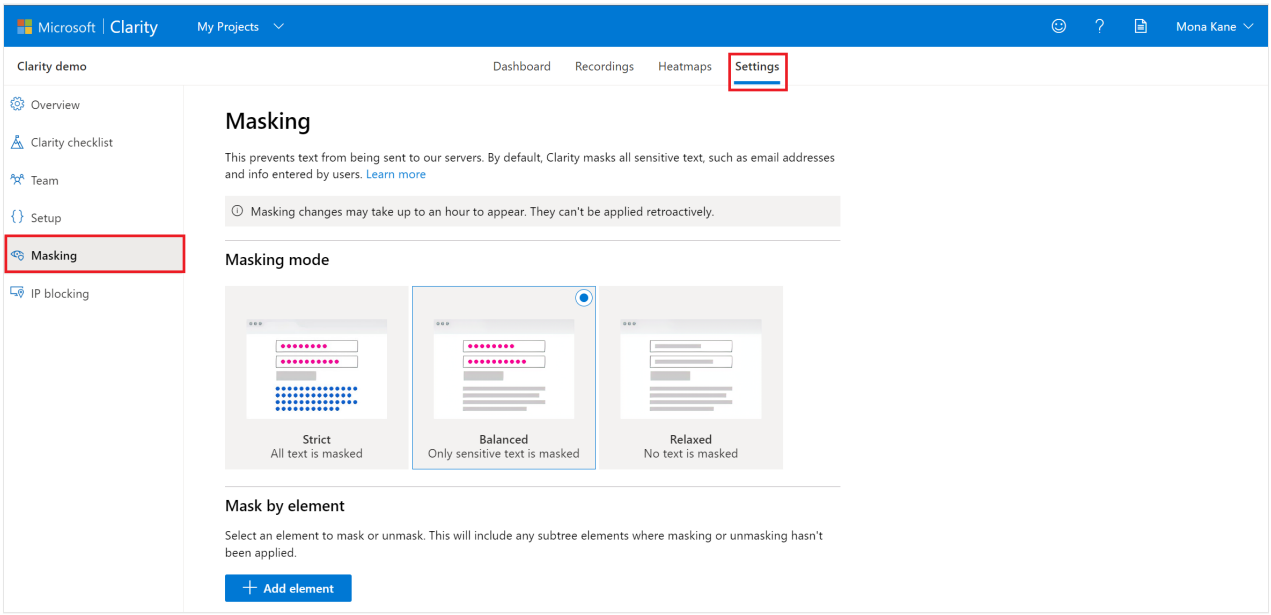
- Mask by element - List the CSS selectors that you want Clarity to mask or unmask. Example of masking by element.
- Using the Clarity data-clarity-mask API - Add an HTML attribute to elements to tell Clarity to mask content.

Using the Clarity website to mask and unmask content

Masking modes

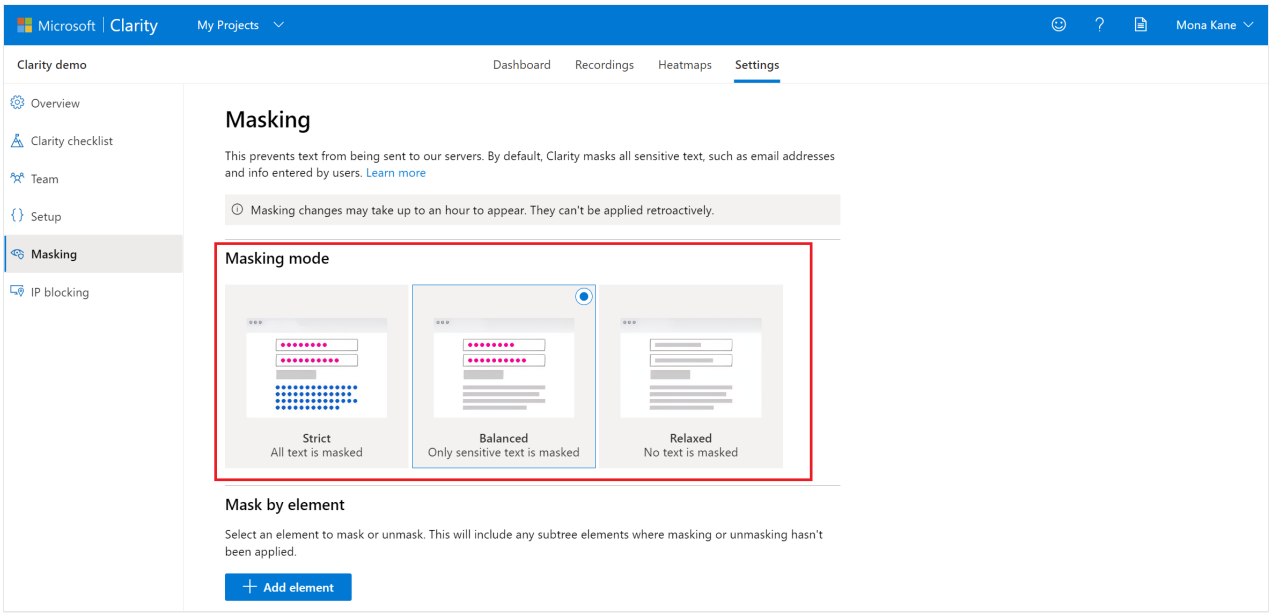
You can easily select one of three masking modes or methods for Clarity to use. By default, the masking mode is set to Balanced.

1. Go to **Settings** > **Masking**.

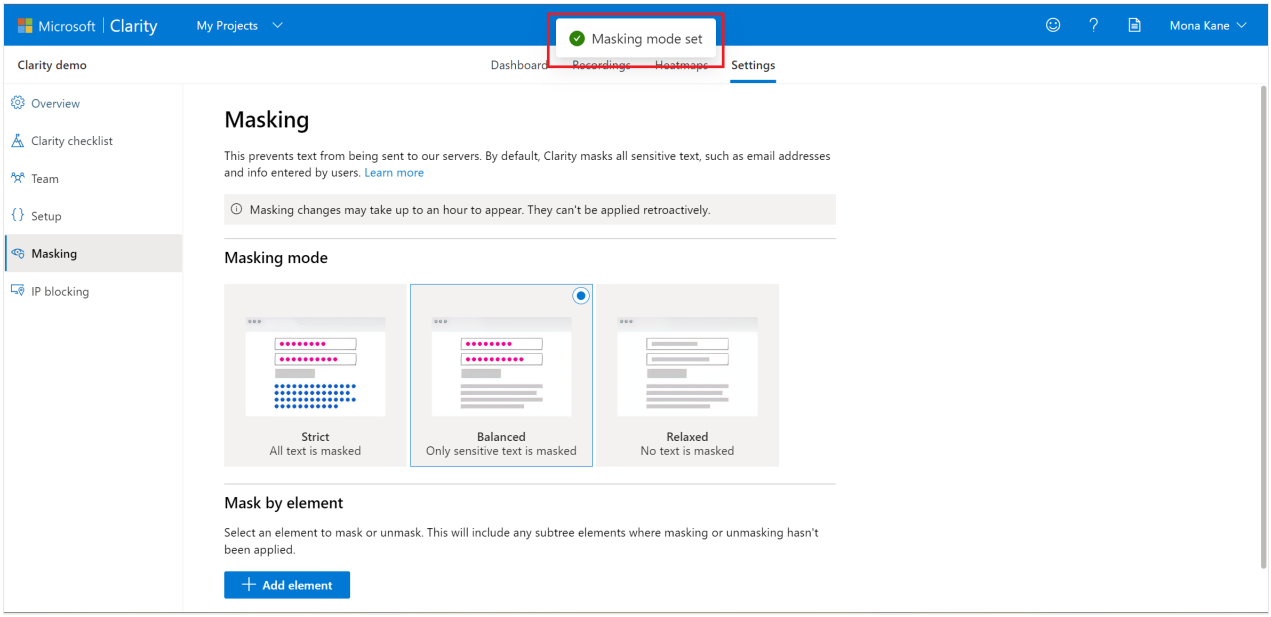


2. Under Masking mode, select a masking mode.

   - **Strict**: The entire text is masked.
   - **Balanced**: Only sensitive text is masked. We classify all input box content, numbers, and email addresses as sensitive text.
   - **Relaxed**: No text is masked.



3. Upon selecting a masking mode, you can view a message as 'Masking mode set' on top of the screen.

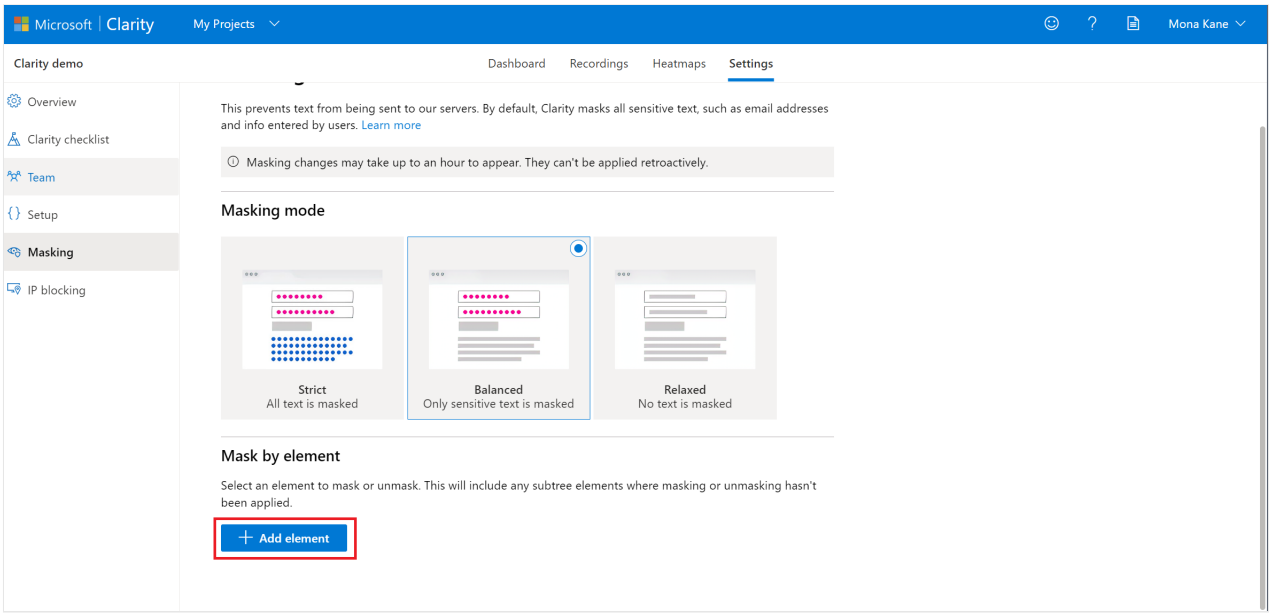


Mask by element

You can also select specific elements to override the overall masking mode of your website. This will affect all its children in the DOM as well.

1. Go to **Settings** > **Masking**.

2. Under Mask by element, select **Add element**.



3. Enter the CSS selector for the element to be marked and select **Confirm**. For example, enter `.class_name` for a class, `#id_value` for an ID, and `element` for a type.

4. As you add the elements, switch between masking and unmasking as you like.

> **Tip**
>
> Check out the **MDN Web Docs** for help with using CSS selectors, including syntax and examples.

5. You can delete an element by selecting the 'Delete' icon.

Using the Clarity `data-clarity-mask` API

Mask content using an HTML element

Mask content by adding `data-clarity-mask="True"` as an attribute on an HTML element in your DOM. That node and its children's contents will be masked. This overrides anything set on the Clarity website.

Unmask content using HTML element

Unmask content by adding `data-clarity-unmask="true"` as an attribute on an HTML element in your DOM. That node and its children's contents will be unmasked. This overrides anything set on the Clarity website.

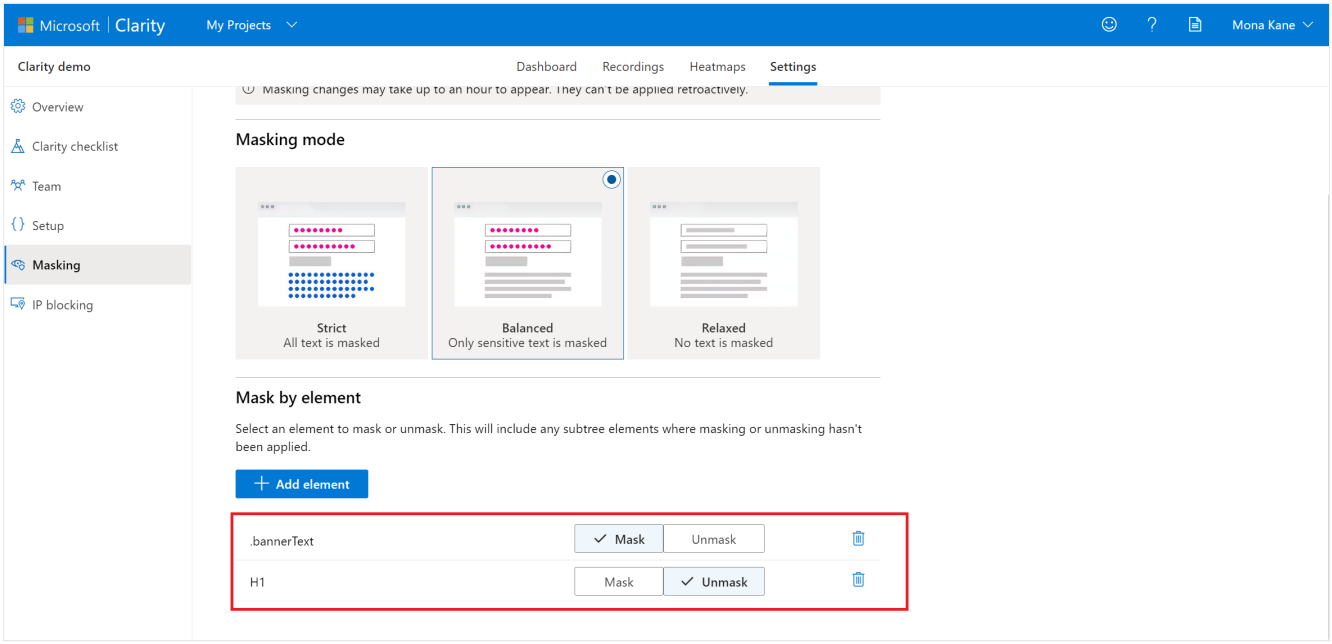
Example of masking by element

HTML elements appear nested within other elements in the DOM of a webpage. Here's how you mask and unmask HTML elements, even if they're nested within each other.

We'll make a small change to masking settings for the Clarity website, inspect the elements in the DOM, and show how the web page rendering in a recording.

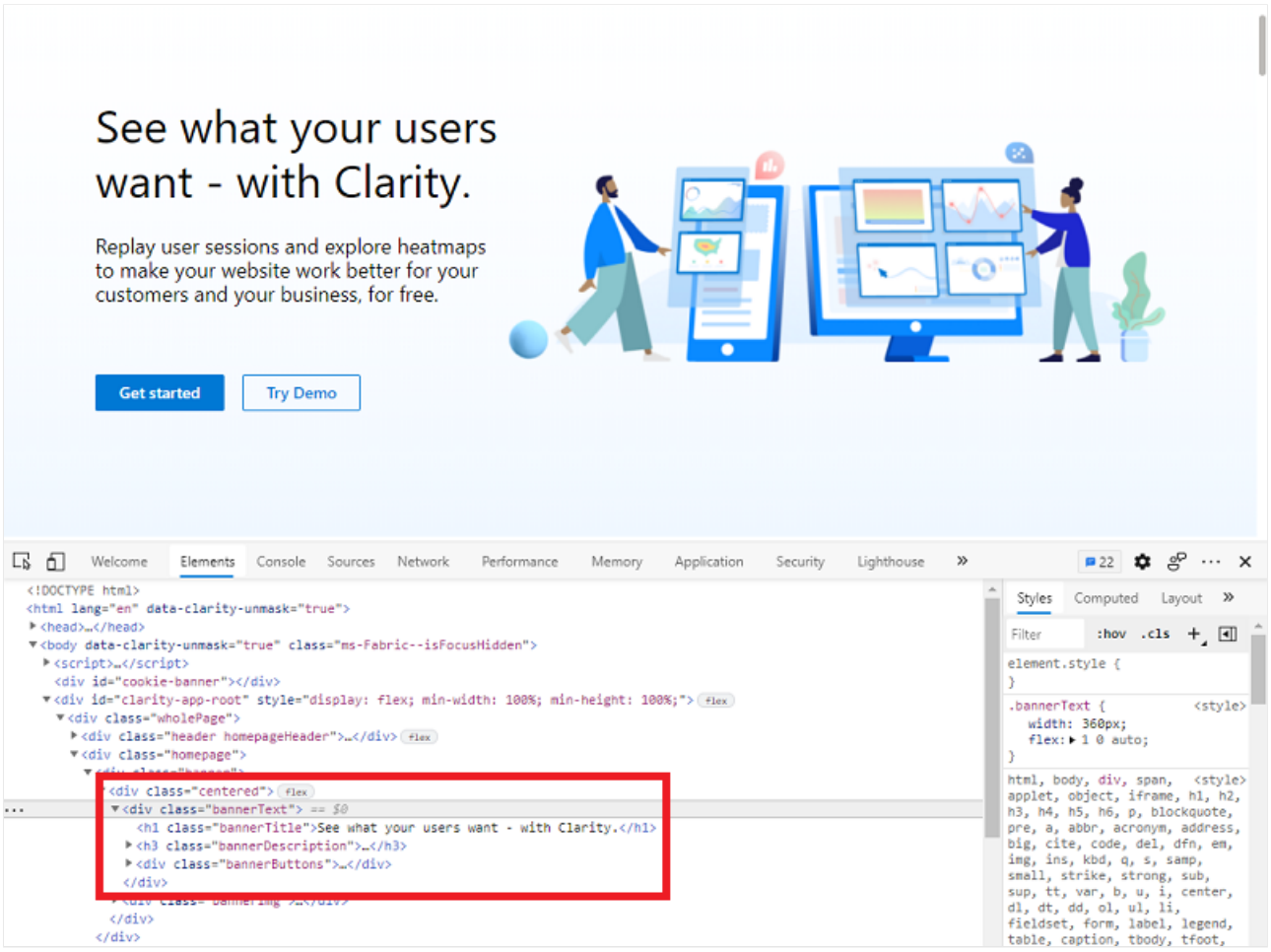
Step 1

On the Masking page of the Clarity website, we set the following values under Mask by element. We entered `.bannerText` for the bannerText class and switched its setting to `Mask`. Similarly, entered `H1` and switched its setting to `Unmask`.



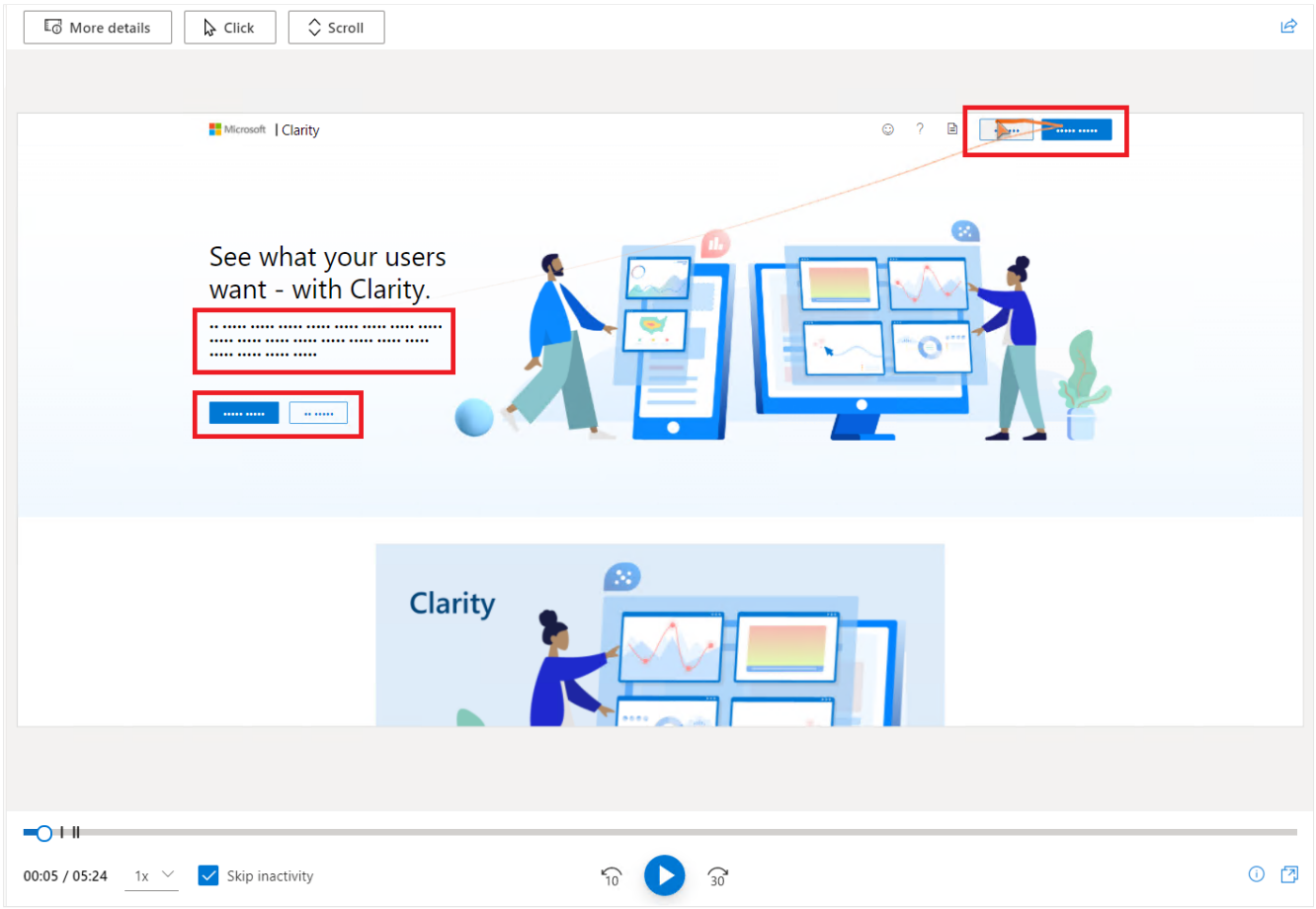
Step 2

Next, we opened the page in the JavaScript console and found the HTML elements. The bannerText class contains three elements in the DOM: `H1`, `H3`, and the `bannerButtons` class. Because `.bannerText` is masked, its `H3` and `bannerButtons` children are masked. However, `H1` is unmasked because it was set to `Unmask` on the Clarity website.



Step 3

About 30 minutes after we changed the Clarity masking settings, we viewed a session for the page under Recordings. The `H1` text, which we set to `Unmask`, is visible, but the `.bannerText` underneath and on `bannerButtons` is masked. These latter elements weren't uploaded to Clarity and can't be seen on recordings.



FAQ

For more answers, refer to Masking and Unmasking FAQ.

Next steps

Session Recordings overview

Heatmaps overview

How to use Clarity on third-party platforms?

Explore more

Team management

Insights overview

Filters in Clarity

Visit Clarity

> Case studies

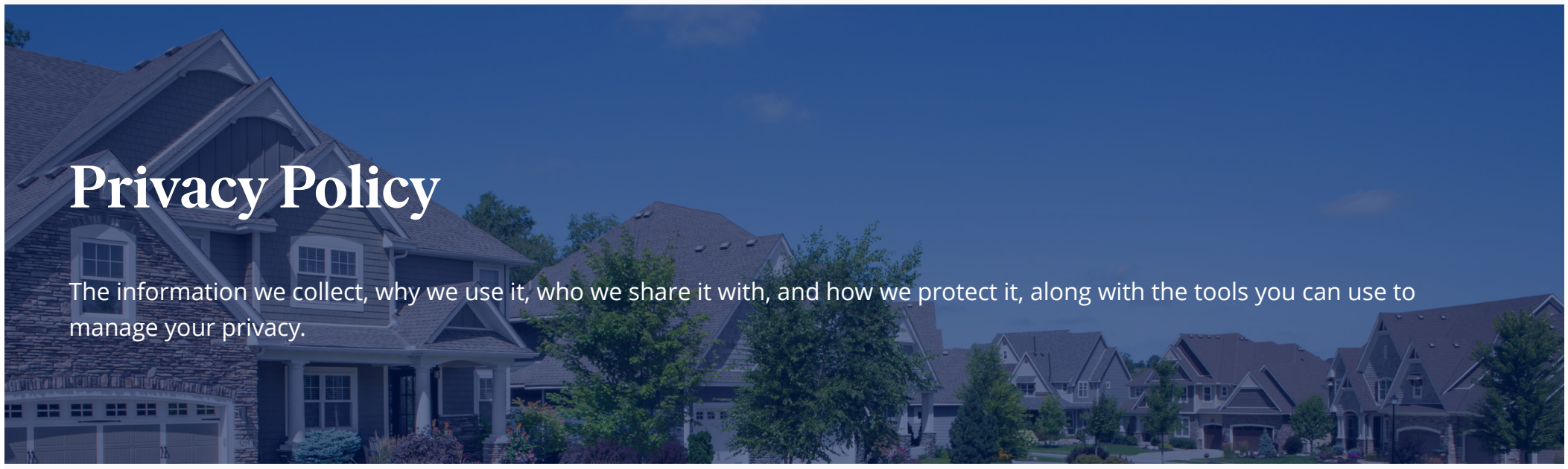
> Demo

> Sign in

> Blog

> Benchmarks

EXHIBIT 3



Privacy Policy

The information we collect, why we use it, who we share it with, and how we protect it, along with the tools you can use to manage your privacy.

Effective Date: January 2023

When you use Zillow Group services to find, buy, rent, or sell your home, get a mortgage, or connect to a real estate pro, we know you're trusting us with your data. We also know we have a responsibility to respect your privacy, and we work hard to do just that. This Privacy Notice explains what personal data we collect, why we use it, who we share it with, and how we protect it, along with the tools you can use to manage your privacy. We periodically revise this Notice to reflect new and evolving laws that govern privacy. This Privacy Notice is not a contract and does not create any legal rights or obligations.

Who We Are: Zillow Group offers a wide range of offerings that focus on all stages of your home journey: searching, renting, buying, selling, financing, and home improvement.

We know that everyone's home journey is different, and that deciding on the right place to call home is an intimate, personal experience. Along with a wealth of information about homes, neighborhoods, market conditions, local real estate professionals, and financing options, we also use the information you give us to provide our services and help you find your next home.

We carefully evaluate how we use data to make sure that we're using your information to provide value **for you**. On this page, we aim to explain everything you need to know about your privacy at Zillow. If you have any questions that we haven't answered here, you can always contact us at privacy@zillow.com.

When we use the terms "Zillow Group", "we", "us", or "our" in this Privacy Notice, we are referring to Zillow, Inc. and its affiliated brands.

Our Offerings: When we use the terms "offerings" or "services," we are referring to our Internet websites, mobile applications, and other services that link to this Privacy Notice and that we offer and manage on our own behalf, including:

- Our corporate websites that link to this Privacy Notice;
- Rental tools;
- Connections (such as connecting you to a lender or agent); and
- Other offerings we may make available through our sites and apps.

This Privacy Notice does not cover or address:

- Our business-facing brands, such as dotloop, ShowingTime, ShowingTime+, Mortech, and Bridge Interactive, all of which have their own Privacy Notices;
- Zillow Home Loans and Zillow Closing Services, each of which has its own Privacy Notice;
- Disclosures or rights we may provide to you in relation to the United States Fair Credit Reporting Act (FCRA) or
- the United States Gramm-Leach-Bliley Act (GLBA);
- Disclosures or rights we may provide to you in relation to U.S. state-specific financial privacy laws;
- Offerings that we provide solely on behalf of our business partners; and
- Personal data and privacy practices relating to job applicants, employees and other Zillow Group personnel.

We separately provide notices required under the GLBA, containing GLBA- and state-specific financial privacy law disclosures in connection with GLBA-covered services. If you would like to obtain another copy of a GLBA notice we previously provided to you, please contact us at privacy@zillow.com.

For offerings provided on behalf of our customers who are real estate professionals (such as real estate agents, builders, third-party lenders, and landlords), please refer to the privacy notice of the real estate professional with whom you have a relationship for information on how they engage us to process your personal data.For individuals based outside the United States and Canada, this Privacy Notice applies solely to their browsing and actions on our website(s) accessible at: www.zillow.com; www.trulia.com; www.hotpads.com; www.zillowgroup.com; www.streeteasy.com, and www.outeast.com.

Quick links

What is Personal Data?

When we use the term "personal data" in this Privacy Notice, we mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an individual or household. It does not include aggregated or de-identified information that is maintained in a form that is not capable of being associated with or reasonably linked to an individual.

Our Collection and Use of Personal Data

The personal data we collect, the way we collect it, and how we use it will depend on how you are interacting with us and the type of services you use.

Information We Collect As You Use Our Services

Collection of Personal Data

As is true of most digital platforms, we and our third-party providers collect certain personal data automatically when you visit or interact with our websites, mobile apps, and other online services. This includes things like your home search history, homes you view, purchase activity, what you've clicked on and other uses of our websites, and the amount of time you spend looking at different parts of our websites.

Specifically, we and our third party partners may use tracking technologies to automatically collect commercial information, preferences, and internet, network and device information, including:

- **Information about how you access our services**, such as the website from which you came and the website to which you are going when you leave our websites, how frequently you access the services, when and whether you open emails or click the links contained in emails, whether you access the services from multiple devices and other actions you take on the services.
- **Information about how you use the services**, such as the pages you visit, the links you click, the ads you view and click on, purchase information and your checkout process, your location when you access or interact with our services, and other similar actions.
- **Information about the computer, tablet, smartphone or other device you use**, such as your IP address, browser type, Internet service provider, platform type, device type/model/manufacturer, operating system, date and time stamp, a unique ID that allows us to uniquely identify your browser, mobile device, or your account

(including, e.g., a persistent device identifier or an Ad ID), and other such information (referred to herein as "Log Data").

- **Analytics Data**, such as information about your activity when you visit our sites or use our apps; this can include clicks, mouse movements, forms you fill out, and similar information. We use this to better understand what features and parts of the website are most useful, and which ones may need to be improved.

- **Cookies, pixels, and other tracking**: We and our partners use various tools to collect data when you visit our sites and apps, including cookies, pixel tags, and other similar technologies. Cookies are bits of electronic data that can be transferred to your computer or other device to identify your browser. When you use Zillow, we and our partners may use cookies and other tools to gather information about how you view and use our services and content, and to connect your activity with other data we store about you. The use of cookies helps us serve you better by understanding what you're interested in, tracking trends, measuring the effectiveness of ads, saving your preferences, and storing information you may want to retrieve on a regular basis, such as your favorite homes. We also allow approved partners to collect data from your browser or device for advertising and measurement purposes using their own cookies or similar tools; these are categorized as "Advertising Cookies," and you can choose whether to disable them via either our Privacy Center or the "Cookie Preference" link at the bottom of our websites.

  This information allows us to improve your customer experience. For example, we may use this information to enhance and personalize your user experience, to monitor and improve our websites and services, and for other internal purposes. We may also use this information to: (a) remember information so that you will not have to re-enter it during your visit or the next time you visit the Sites; (b) provide custom, personalized content, and information; (c) identify and contact you across multiple devices; (d) provide and monitor the effectiveness of our services; (e) perform analytics and detect usage patterns on our services; (f) diagnose or fix technology problems; (g) detect or prevent fraud or other harmful activities; and (h) otherwise to plan for and enhance our services.

  We and our third party partners may collect information through tracking technologies for personalized advertising purposes. To learn more about our advertising practices and your choices relating to advertising, please see "Third-Party Tracking and Interest-Based Advertising."

  Information You Give Us or Create Using Our Services

  Collection of Personal Data

  When you use our services, websites, or apps, we collect personal data from you. We might also collect personal data about you from our business partners, payment processors, service providers, and other third parties who collect personal data on our behalf. This information might include:

- **Account Registration and Profile Information**: If you register for an account through our services or complete a Zillow profile, we collect account identifiers (including a username and password, as well as internal identifiers we assign to individual accounts to allow our systems to connect account information stored in different databases) and account history and records (including services you've used or interacted with, the date and type of account creation, account status, log in activity, transactions, the services we provide, messages received in connection with the services, and your activity on our websites and mobile applications). We use this information to create and administer your account, provide you with the relevant services and information, communicate with you regarding your account and your use of the services, for customer support purposes, and to send you communications by email, push notification, or by text message, in accordance with your preferences.
- **Customer Service and Communication History**: Including name, address, email, customer service requests, Account Identifiers, Account History and the contents of requests and correspondence with us (including recordings of phone calls, where permitted by law).
- **Feedback Information**: If you submit a review, feedback or other comments, we collect your contact information (such as first and last name, email address, and phone number) and any feedback and ratings relating to our services and products, including reviews you create of real estate pros.
- **Inquiries and Communication**: If you communicate with us or otherwise submit an inquiry or question (e.g., via webform), we collect your contact information (such as first and last name, email address, and phone number), account identifiers and history (described above), and any other personal data you choose to provide in the content of your message or communication. We use this information to investigate and respond to your inquiries, to facilitate communication with us, to provide you with requested information, to enhance the services we offer, and to manage and grow our business. If you represent a company or agency interested in partnering with us, we will also collect your professional and employment information in order to respond to your inquiries, communicate with you, to manage and grow our organization and to facilitate a business relationship. Our websites and online services provide you the ability to connect with us through an online web form that collects contact information (such as first and last name, email address, phone number, company name, and title with company), area(s) of interest or concern, and a custom message.

- **Location Data**: Including general geographic location reflected in the Log Data we collect or more precise location when you choose to share it with us through your device or browser settings.
- **Newsletters and Email Communication**: Many of our websites and online services provide you an opportunity to sign up for our newsletters and email communications by providing your email address. We use your email address to communicate with you about our services and exciting developments at Zillow Group, which may include marketing communications. Please see the "Choices About Your Data" section below for additional information about opting out of our marketing communications.
- **Payment Information**: We and our third-party service providers collect information relating to your transactions with us, including details regarding payments you've made through our sites or apps. We use third-party payment tools to process and store payment information like credit card numbers or bank account information. We don't store this information ourselves.

Although we often collect the personal data described above directly from you, we may also collect certain information through our business partners, service providers, and other third parties that collect it on our behalf, such as communications providers, data brokers, payment processors, payment system providers, and information technology providers.

Please note that we link the personal data we collect in connection with our services with the other personal data that we collect and may use it for the purposes we describe in more detail in the other sections of this Privacy Notice.

Other Collection of Personal Data

In addition to the personal data collected above, we may also collect personal data as follows:

- **Affiliates**: We may receive information about you collected by other Zillow Group companies, businesses, brands, and affiliated entities in our family of companies, so that information you provide to one brand may be used by us to better provide you services and communicate with you.
- **Business Partners**: Our business partners, such as agent partners, lending partners, builders, property managers, and other real estate professionals collect personal data in connection with their services and often share some or all of this information with us. For example, we receive information about transactions you complete with partners with whom we've connected you through our services.
- **Business Representatives**: We collect professional personal data about representatives of third-party businesses, including representatives of our customers and business partners, in connection with our services and the operation of our business, which may include:
  - *Contact Information*: Including full name, email address, mailing address, and telephone number.
  - *Professional Information*: Including job title, job function, company name and characteristics, professional background, and nature of the relationship with us.
  - *Tax and Payment Information*: Including a personal tax identification number, bank account information, and payment information where you are a representative of a sole proprietor or similar legal structure that uses personal tax and account information in lieu of separate business information.
  - *Inquiry Information*: Including the contents of emails, texts, and other communications and, where permitted by law, recordings of calls with us.
  - *Feedback Information*, including information provided in response to surveys we may conduct with customers or business partners, or unsolicited feedback received regarding our services and business.
- **Office and Event Visitors**: We collect personal data about visitors to our physical offices and events, which may include:
  - *Contact Information*: Including full name, email address, mailing address, and telephone number.
  - *Professional Information*: Including job title, job function, company name, professional background, and nature of the relationship with us.
  - *Visit Information*: Including the purpose of the visit and any restrictions or preferences while on premise (such as dietary restrictions).
  - *Security Information*: Including a copy of a government ID (such as a driver's license) and a record of the visitor's access to our office or event, any use by the visitor of our computer systems, and images or video recordings of the visitor while on premises (where permitted by law).
- **Service Providers**: Our service providers, such as payment processors and marketing providers, collect personal data and often share some or all of this information with us. For example, we receive personal data from payment processors to confirm that an individual's payment for the services was accepted. We use this information to comply with our legal obligations, to monitor activity to identify and provide you with promotions and offers, and to prevent fraud, protect our rights and the rights of others, to inform our marketing and advertising activities, and to help provide our services.
- **Information Providers**: We may from time to time obtain information from third-party information providers to correct or supplement personal data we collect. For example, we may obtain updated contact information from third-party information providers to reconnect with you.

- **Publicly Available Information**: We may collect personal data from publicly available sources, such as information you publicly post or tag us in on social media sites or elsewhere online, and information contained in public records databases, such as government records or public review websites, to supplement the personal data identified above. We will use this information to conduct market research, verify your identity, prevent fraud, and improve our services.

Other Uses of Personal Data

In addition to the uses identified above, we use the personal data we collect to:

- Facilitate our day-to-day business operations, such as helping you find your next home, or connect with a real estate agent, lender, landlord, or other real estate professional;
- Create and maintain the services, develop new products and services, and improve existing products and services;
- Aggregate information we receive from you and third parties to help understand individual needs, customize our services and offerings, and provide everyone better service;
- Conduct research and analytics designed to understand our customer base and improve and grow our business, products, services, and customer experience;
- Communicate with you to provide technical or administrative support;
- Prevent, investigate, and defend against fraud or unlawful or criminal activity, access to, or use of personal data and our data system services;
- Enforce, investigate, and resolve disputes and security issues and to enforce our Terms of Service and any other contracts;
- Comply with legal obligations and other governmental demands;
- Understand your preferences and interests to better serve you on your home-finding journey;
- Personalize your individual experience, including providing educational resources and pointing you to homes you might be interested in or offerings of ours that might help you find your next home; and
- For any other lawful, legitimate business purpose.

Our Disclosure of Personal Data

We may disclose your personal data in the instances described below. For further information on your choices regarding your information, see the "Choices About Your Data" section below.

We disclose your personal data in the following ways:

- **Within Zillow Group**: We are able to offer the products and services we make available because of the hard work of the entire Zillow Group team. Zillow Group entities disclose your personal data to other Zillow Group entities for purposes and uses that are consistent with this Privacy Notice and applicable law. For example, one part of Zillow might share your personal data with another in order to ensure that all the people helping in your home journey are working together for you.
- **Business Partners**: At your direction, we may share your personal data with our business partners in order to provide you with our products and services. For example, if you ask us to, we'll share your contact information with a real estate agent or mortgage lender.
- **Marketing Partners**: We coordinate and share your personal data with our marketing partners, including advertising networks, social networks, and marketing communication providers, in order to communicate with you about our products and services and market our products and services to you. We may also share aggregated demographic information with third parties interested in advertising on our online services to assist them in understanding the audience they would be reaching, but this information is not designed to identify any specific individual.
- **Service Providers**: We share information with third party vendors and service providers that perform services for or on our behalf, which may include identifying and serving targeted advertisements, providing mailing or email services, tax and accounting services, customer service, product fulfillment, payments processing, photo sharing, data processing and enhancement services, fraud prevention, web hosting, analytic services, or other online functionality, subject to appropriate contractual terms protecting the confidentiality and use of such data. We never allow service providers to use your personal data for their own purposes.
- **Business Transaction or Reorganization**: We may take part in or be involved with a corporate business transaction, such as a merger, acquisition, joint venture, or financing or sale of company assets. We may disclose your personal data to a third party during negotiation of, in connection with, or as an asset in such a corporate business transaction. Your personal data may also be disclosed in the event of insolvency, bankruptcy, or receivership.
- **Legal Obligations and Rights**: We may disclose your personal data to third parties, such as legal advisors and law enforcement:
    - In connection with the establishment, exercise, or defense of legal claims;
    - To comply with laws and regulations or to respond to lawful requests and legal process;

- To protect our rights and property and the rights and property of our agents, customers, and others, including to enforce our agreements, policies, and terms of use;
- To detect, suppress, or prevent fraud;
- To reduce credit risk and collect debts owed to us;
- To protect the health and safety of us, our customers, or any person; or
- As otherwise required by applicable law.
- For Zillow's policy on government and civil requests for information, please see Government and Civil Information Requests.

- **Otherwise with Consent or At Your Direction**: We may disclose your personal data to certain other third parties or publicly with your consent or direction. If you post a comment or review our website or a comment on our social media sites, the information you provide may be displayed publicly online for others to view.

Choices About Your Data

Profile Access and Data Sharing. You may access and update your profile information, such as your user name, address, or billing information, and may change some of your data sharing preferences on your account page.

Location and Device Permissions. You may control location tracking by adjusting your location services options on the "Settings" app on your mobile device. We may continue to approximate your location based on your IP address when you access the services through a computer or device. If you would like to update your device content access permissions, such as permissions to access your camera, you can do so in the "Settings" app on your mobile device.

Promotional Messages. You can stop receiving promotional email communications from us by following the "unsubscribe" instructions provided in such communications. We make every effort to promptly process all unsubscribe requests. You may still receive service-related communications, including account verification, transactional communications, changes/updates to features of the services, and technical and security notices.

Third Party Tracking and Interest-Based Advertising. We participate in interest-based advertising and use third party advertising companies to serve you targeted advertisements based on your browsing history. To learn more about our advertising practices and your choices relating to advertising, please see "Third-Party Tracking and Interest-Based Advertising."

Third-Party Tracking and Interest-Based Advertising

We may participate in interest-based advertising and use third party advertising companies to serve you targeted advertisements based on your browsing history. We may permit third party online advertising networks, social media companies, and other third-party services to collect information about your use of our websites, including our mobile apps, over time so that they may play or display ads on our services, on other websites, apps, or services you may use, and on other devices you may use. Typically, though not always, the information used for interest-based advertising is collected through tracking technologies, such as cookies, Flash objects, web beacons, embedded scripts, mobile SDKs, location-identifying technologies, and similar technology (collectively, "tracking technologies"), which recognize the device you are using and collect information, including clickstream information, browser type, time and date you visited the site, device ID or AdID, geolocation, and other information. We may share a common account identifier (such as an e-mail address or user ID) or hashed data with our third-party advertising partners to help identify you across devices. We and our third-party partners may use this information to make the advertisements you see online more relevant to your interests, as well as to provide advertising-related services such as reporting, attribution, analytics, and market research.

We, or our third-party partners, may link your various devices so that content you see on one device can result in relevant advertising on another device. We may share a common account identifier (such as a hashed email address or user ID) or work with third-party partners who use tracking technologies or statistical modeling tools to determine if two or more devices are linked to a single user or household. We, and our partners, can use this cross-device linkage to serve interest-based advertising and other personalized content to you across your devices (including to improve your user experience), to perform analytics, and to measure the performance of our advertising campaigns.

Your Choices

As noted above, depending on your browser or mobile device, you may be able to set your browser to delete or notify you of cookies and other tracking technology by actively managing the settings on your browser or mobile device. You may be able to limit interest-based advertising through the settings on your mobile device by selecting "limit ad tracking" (iOS) or "opt-out of interest based ads" (Android). Please note that opt-outs are browser specific, so opting out on one browser will not affect a second browser, or device. Moreover, if you buy a new device, use a different browser, or clear all your cookies, you will have to opt out all over again. To learn more about interest-based advertising and how you may be able to opt-out of some of this advertising, you may

wish to visit the Network Advertising Initiative's online resources, at http://www.networkadvertising.org/choices, and/or the DAA's resources at www.aboutads.info/choices. You may also be able to opt-out of some – but not all – interest-based ads served by mobile ad networks by visiting http://youradchoices.com/appchoices and downloading the mobile AppChoices app. Note that some of these opt-outs may not be effective unless your browser is set to accept cookies. If you delete cookies, change your browser settings, switch browsers or computers, or use another operating system, you may need to opt-out again.

Children's Personal Data

Our websites and online services are not directed to, and we do not intend to or knowingly collect or solicit personal data from children under the age of 13. If you are under the age of 13, please do not use our websites or online services or otherwise provide us with any personal data either directly or by other means. If a child under the age of 13 has provided personal data to us, we encourage the child's parent or guardian to contact us as described below to request that we remove the personal data from our systems. If we learn that any personal data we collect has been provided by a child under the age of 13, we will promptly delete that personal data.

Region-Specific Disclosures

We may choose or be required by law to provide different or additional disclosures relating to the processing of personal data about residents of certain countries, regions, or states. Please see below for disclosures that may be applicable to you:

- If you are a resident of the State of California, Colorado, Connecticut, Utah, or Virginia in the United States, please see below for additional U.S. state-specific privacy disclosures.
- If you are a resident of the State of Nevada in the United States, Chapter 603A of the Nevada Revised Statutes permits a Nevada resident to opt out of potential future sales of certain covered information that a website operator has collected or will collect about the resident. To submit such a request, please contact us at privacy@zillow.com.

Third-Party Websites

Our websites and online services may include links to or redirect you to third-party websites, plug-ins and applications, including social media services where you may connect with us. Third-party websites may also reference or link to our websites and online services. Except where we post, link to, or expressly adopt or refer to this Privacy Notice, this Privacy Notice does not apply to, and we are not responsible for, any personal data practices of third-party websites and online services or the practices of other third parties. To learn about the personal data practices of these third parties, please visit their respective privacy notices or policies.

Updates to this Privacy Notice

We will update this Privacy Notice from time to time. When we make changes to this Privacy Notice, we will change the "Last Updated" date at the beginning of this Privacy Notice. If we make material changes to this Privacy Notice, we will notify you. All changes shall be effective from the date of publication unless otherwise provided in the notification.

Contact Us

If you have any questions or requests in connection with this Privacy Notice or other privacy-related matters, please send an email to privacy@zillow.com.

Alternatively, inquiries may be addressed to:

Zillow, Inc.
Attn: Consumer Care
1301 Second Avenue

Floor 31
Seattle, WA 98101

Additional U.S. State Privacy Disclosures

These Additional U.S. State Privacy Disclosures supplement the above information by providing additional information about our personal data processing practices relating to individual residents of the States of California, Colorado, Connecticut, Utah, and Virginia. Unless otherwise expressly stated, all terms defined in our Privacy Notice retain the same meaning in these Disclosures.

Additional Personal Data Disclosures

Sensitive Information

The following personal data elements we collect may be classified as "sensitive" under certain privacy laws ("sensitive information"):

- Social Security number, driver's license number, and passport number;
- Credit/debit card number plus expiration date and security code (CVV), and financial account number and routing number;
- Username and password; and
- Precise geolocation data.

We use this sensitive information for the purposes set forth in the "Our Collection and Use of Personal Data" section of our Privacy Notice, to enter into and perform a contract with you, to comply with legal and regulatory requirements, to protect the life or physical safety of you or others, or as otherwise permissible for our internal business purposes consistent with applicable laws.

We do not sell your sensitive information, and we do not process or otherwise share sensitive information for the purpose of targeted advertising.

De-identified Information

We may at times receive or process personal data to create de-identified data that can no longer reasonably be used to infer information about, or otherwise be linked to, a particular individual or household. Where we maintain deidentified data, we will maintain and use the data in de-identified form and not attempt to re-identify the data except as required or permitted by law.

Your Privacy Choices

Depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to exercise some or all of the following rights:

The Right to Know	The right to confirm whether we are processing your personal data and, under some state laws, to obtain certain personalized details about the personal data we have collected about you, including: The categories of personal data collected; The categories of sources of the personal data; The purposes for which the personal data were collected; The categories of personal data disclosed to third parties (if any), and the categories of recipients to whom the personal data were disclosed; The categories of personal data shared for cross-context behavioral advertising purposes (if any), and the categories of recipients to whom the personal data were disclosed for those purposes; and The categories of personal data sold (if any), and the categories of third parties to whom the personal data were sold.data and, under some state laws, to obtain certain personalized details about the personal data we have collected about you, including:The categories of personal data collected;The

	categories of sources of the personal data;The purposes for which the personal data were collected; The categories of personal data disclosed to third parties (if any), and the categories of recipients to whom the personal data were disclosed;The categories of personal data shared for cross-context behavioral advertising purposes (if any), and the categories of recipients to whom the personal data were disclosed for those purposes; andThe categories of personal data sold (if any), and the categories of third parties to whom the personal data were sold.
The Right to Access & Portability	The right to obtain access to the personal data we have collected about you and, where required by law, the right to obtain a copy of the personal data in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another entity without hindrance.
The Right to Correction	The right to correct inaccuracies in your personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data.

The Right to Deletion	The right to have us delete the personal data we maintain about you.
The Right to Opt-Out of Sales or Sharing of Personal Data	The right to direct us not to "sell" your personal data to third parties for monetary or other valuable consideration, or "share" your personal data to third parties for cross-context behavioral advertising purposes and targeted advertising purposes.
"Shine the Light"	California residents that have an established business relationship with us have rights to know how their personal data is disclosed to third parties for their direct marketing purposes under California's "Shine the Light" law, or the right to opt out of such practices (Civ. Code §1798.83).

Depending on your state of residence, you may also have the right to not receive retaliatory or discriminatory treatment in connection with a request to exercise the above rights. However, the exercise of the rights described above may result in a different price, rate, or quality level of product or service where that difference is reasonably related to the impact the right has on our relationship or is otherwise permitted by law.

Submitting Privacy Rights Requests

To submit a request to exercise one of the privacy rights identified above, please:

- Navigate to our **Privacy Center**; or
- Email us at privacy@zillow.com.

We may need to verify your identity before processing your request. In order to submit a request, you'll need to log in to your account with us so we can verify your identity. If you can't log in or don't have an account, we may not be able to link you to any personal data of yours on our systems, but we'll do our best. In certain circumstances, we may decline a request to exercise the rights described above, particularly where we are unable to verify your identity or locate your information in our systems. We will use personal data provided in connection with a Rights Request only to review and comply with the request.

To Exercise Your Right to Opt-Out of Personal Data Sales or Sharing for Targeted Advertising

Unless you have exercised your Right to Opt-Out, we may disclose your personal data to third parties who may use such information for their own purposes in accordance with their own privacy policies. Under some state laws, disclosing personal data for online advertising like this may be considered a "sale of personal data" or "sharing for targeted advertising."

Zillow allows certain companies to place tracking technologies like cookies and pixels on our sites, which allow those companies to receive information about your activity on Zillow that is associated with your browser or device. The companies may use that data to serve you more relevant ads on our sites or others. Except for this kind of selling or sharing, Zillow doesn't otherwise sell any of your personal data. You always have control over whether these technologies work on your devices. At any time, you can use our cookie preference tools to manage what kinds of cookies and other tracking technologies you're comfortable with. Check out our Privacy Center for information about how to access these tools. You can also disable cookies altogether by adjusting the settings on your browser. However, if you choose to disable some or all cookies, many parts of our services may no longer work. For more information, see the "Third-Party Tracking and Interest-Based Advertising" section in the Privacy Notice.

You do not need to create an account with us to exercise your Right to Opt-Out. However, we may ask you to provide additional personal data so that we can properly identify you to track compliance with your opt-out request. We will only use personal data provided in an opt-out request to review and comply with the request. If you choose not to provide this data, we may be able to process your request only to the extent we are able to identify you in our data systems.

To exercise the Right to Opt Out of Personal Information Sales or Sharing: Navigate to our **Privacy Center** or email privacy@zillow.com with sufficient information to identify you and your request.

Submitting Authorized Agent Requests

In certain circumstances, you are permitted by law to use an authorized agent to submit requests on your behalf through the designated methods set forth above where we can verify the authorized agent's authority to act on your behalf. In order to verify the authorized agent's authority, we generally require evidence of either: (i) a valid power of attorney; or (ii) a signed letter containing your name and contact information, the name and contact information of the authorized agent, and a statement of authorization for the request. Depending on the evidence provided and your state of residence, we may still need to separately reach out to you to confirm the authorized agent has permission to act on your behalf and to verify your identity in connection with the request.

Appealing Privacy Rights Decisions

Depending on your state of residence, you may be able to appeal a decision we have made in connection with your privacy rights request. All appeal requests should be submitted via email to privacy@zillow.com.

Minors

We do not sell the personal data of consumers we know to be less than 16 years of age, unless we receive affirmative authorization (the "Right to Opt In") from either the minor who is between 13 and 16 years of age, or the parent or guardian of a minor less than 13 years of age.

If you are under the age of 18 and you want to remove your name or comments from our website or publicly displayed content, please contact us directly at privacy@zillow.com. We may not be able to modify or delete your information in all circumstances.

If you wish to submit a privacy request on behalf of your minor child in accordance with applicable jurisdictional laws, you must provide sufficient information to allow us to reasonably verify your child is the person about whom we collected personal information and you are authorized to submit the request on your child's behalf (i.e., you are the child's legal guardian or authorized representative).

California-Specific Disclosures

The following disclosures only apply to residents of the State of California.

California Categories of Personal Data

California law requires we provide disclosures to you about what personal data we collect by reference to the enumerated categories of personal data set forth within California law. To address this obligation, we have identified the relevant enumerated California personal data category for the personal data, sources and purposes described in the "Our Collection and Use of Personal Data" section of our Privacy Notice below:

- **Identifiers**, including Account Registration and Profile Information, information related to your feedback, inquiries, and communications, credit and identity information relating to data used to identify you, full name, IP

address, and government identification number (including Social Security number, passport number, and driver's license number).

- **Customer Records**, including Account Registration and Profile Information, Security/Authentication Information, and Payment Information.
- **Protected Classification Characteristics**, including age, date of birth, gender, and sex.
- **Commercial Information**, including Account Registration and Profile Information relating to your purchases, Profile Information relating to your transactions, preferences, and interests, and Feedback Information.
- **Internet/Network Information**, including information about how you access and use the services, Log Data, and Analytics Data.
- **Geolocation Data,** including general geographic location or more precise location with your consent or when permitted by law.
- **Sensory Information**, including, where permitted by law, recordings of phone calls between us and individuals, and image and video recordings of visitors to our offices or events.
- **Profession/Employment Information**, including the business or organization you represent, your title with that business or organization, and information relating to your role with the business or organization.
- **Sensitive Information**, including Social Security number, driver's license number, passport number, credit/debit card number plus expiration date and security code (CVV), financial account number and routing number, username and password, and precise geolocation.
- **Other Personal Data**, including any information you provide us in connection with signing up for newsletters, email communications, and surveys, personal data you permit us to see when interacting with us through social media, and personal data you provide us in relation to a question, request, inquiry, survey, contest, or promotion.
- **Inferences**, including our predictions about interests and preferences and related Service Profile Information.

We collect this data from the following sources: directly from you, from our business partners and affiliates, from your browser or device when you visit our mobile app(s) or use our Services, or from third parties that you permit to share information with us. Please see "Our Collection and Use of Personal Data" section of our Privacy Notice for more information about the sources of personal data we collect. We disclose all of these categories of personal data for a business purpose to service providers or other third parties at the consumer's direction, as outlined in the "Our Disclosure of Personal Data" section of our Privacy Notice.

Retention of Personal Data

We strive to retain your personal data only for as long as is reasonably necessary to fulfill the purpose for which it was collected. However, if necessary, we may retain your personal data for longer periods of time, until set retention periods and deadlines expire, for instance where we are required to do so in accordance with legal, tax and/or accounting requirements set by a legislature, regulator, or other government authority.

To determine the appropriate duration of the retention of personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of personal data and if we can attain our objectives by other means, as well as our legal, regulatory, tax, accounting, and other applicable obligations.

Therefore, we retain personal data for as long as you use our services for the purposes explained in our Privacy Notice, including maintaining a user account. When you discontinue the use of our services, we will retain your personal data for as long as necessary to comply with our legal obligations, to resolve disputes and defend claims, as well as for any additional purpose based on the choices you have made, such as to receive marketing communications.

Once retention of your personal data is no longer necessary for the purposes outlined above, we will either delete or de-identify the personal data or, if this is not possible (for example, because personal data has been stored in backup archives), then we will securely store your personal data and isolate it from further processing until deletion or deidentification is possible.

"Shine the Light" Disclosures

The California "Shine the Light" law gives residents of California the right under certain circumstances to request information from us regarding the manner in which we share certain categories of personal information (as defined in the Shine the Light law) with third parties for their direct marketing purposes. To opt out of this type of sharing, please visit our Privacy Center or email us at privacy@zillow.com.

*Consumer Rights Metrics 2021*You can find data that reflects the California consumer rights requests that we have processed in the 2021 calendar year (January 2021 – December 2021) by clicking here.

See our previous Privacy Policies:

Effective March 7, 2022

Effective January 1, 2020

Effective June 25, 2019

ZILLOW GROUP

About Us

Media Room

Investors

Careers

Privacy Policy

Terms of Use

Our Brands

- Zillow
- Trulia
- StreetEasy
- Hotpads
- Zillow Rentals
- Zillow Premier Agent
- Zillow Home Loans
- Zillow Closing Services
- ShowingTime+

Our Blogs

- Corporate
- Consumer
- Research
- Tech
- Mortgage Learning
- Agent Resources
- Landlord Resources

Follow Us